Industrial Wireless
Access Point / Bridge / Client

User Manual IE-WL-AP-BR-CL-ABG

1243290000/00/05.11

First Edition, May 2011

Weidmüller

User Manual IE-WL-AP-BR-CL-ABG

The software described in this manual is furnished under a license agreement and may be used only in accordance with the terms of that agreement.

Copyright Notice

Copyright ©2011 Weidmüller Interface GmbH & Co. KG
All rights reserved.
Reproduction without permission is prohibited.

Disclaimer

Information in this document is subject to change without notice and does not represent a commitment on the part of Weidmüller.

Weidmüller provides this document as is, without warranty of any kind, either expressed or implied, including, but not limited to, its particular purpose. Weidmüller reserves the right to make improvements and/or changes to this manual, or to the products and/or the programs described in this manual, at any time.

Information provided in this manual is intended to be accurate and reliable. However, Weidmüller assumes no responsibility for its use, or for any infringements on the rights of third parties that may result from its use.

This product might include unintentional technical or typographical errors. Changes are periodically made to the information herein to correct such errors, and these changes are incorporated into new editions of the publication.

Contact Information

Weidmüller Interface GmbH & Co. KG
Postfach 3030
32760 Detmold
Klingenbergstraße 16
32758 Detmold
Germany

Phone +49 (0) 5231 14-0
Fax +49 (0) 5231 14-2083
E-Mail info@weidmueller.com
Internet www.weidmueller.com

Table of Contents

1. Introduction 1-1
- Overview 1-2
- Package Checklist 1-2
- Product Features 1-2
- Product Specifications 1-3
- Functional Design 1-5
  - LED Indicators 1-5
  - Beeper 1-6
  - Reset Button 1-6
  - Relay (Digital Output) 6

2. Getting Started 2-1
- First-time Installation and Configuration 2-2
- Communication Testing 2-3
- Function Map 2-5

3. Web Console Configuration 3-1
- Web Browser Configuration 3-2
- Overview 3-3
- Basic Settings 3-4
  - System Info Settings 3-4
  - Network Settings 3-5
  - Time Settings 3-6
- Wireless Settings 3-7
- Operation Mode 3-8
- Basic Wireless Settings 3-8
  - WLAN Security Settings 3-11
  - Advanced Wireless Settings 3-18
  - WLAN Certification Settings (for EAP-TLS in Client mode only) 3-22
- Advanced Settings 3-23
  - Using Virtual LAN 3-23
  - Configuring Virtual LAN 3-24
  - DHCP Server (for AP mode only) 3-25
  - Packet Filters 3-26
  - RSTP Settings (for AP mode only) 3-28
  - SNMP Agent 3-30
  - Link Fault Pass-Through (for Client/Slave mode only) 3-32
- Auto Warning Settings 3-32
  - System Log 3-33
  - Syslog 3-33
  - E-mail 3-34
  - Relay 3-36
  - Trap 3-36
- Status 3-38
  - Associated Client List (for AP mode only) 3-38
  - DHCP Client List (for AP mode only) 3-38
  - System Log 3-39
  - Relay Status 3-40
  - DI and Power Status 3-40
  - Wireless Status 3-41
- Maintenance 3-41
  - Console Settings 3-41
  - Ping 3-42
  - Firmware Upgrade 3-42
  - Config Import Export 3-43
  - Load Factory Default 3-43
  - Password 3-44
  - Misc. Settings 3-44
- Save Configuration 3-44
- Restart 3-45
- Logout 3-46

4. Software Installation and Configuration 4-1
- WLAN Administration Tool 4-2
  - Installing WLAN Administration Tool 4-2
  - Configuring WLAN Administration Tool 4-4

5. Other Console Considerations 5-1
- RS-232 Console Configuration (115200, None, 8, 1, VT100) 5-2
- Configuration by Telnet and SSH Consoles 5-4
- Configuration by Web Browser with HTTPS/SSL 5-4

Disabling Telnet and Browser Access 6-5

A. References A-1

Wireless Distribution System (WDS) A-2
Beacon A-3
DTIM A-3
Fragment A-3
RTS Threshold A-3
STP and RSTP A-4
The STP/RSTP Concept A-4
Differences between RSTP and STP A-4

B. Supporting Information B-1

About This User's Manual B-2
DoC (Declaration of Conformity) B-2
Federal Communication Commission Interference Statement B-2
R&TTE Compliance Statement B-3

1

Introduction

The IE-WL-AP-BR-CL-ABG enables wireless users to access network resources wirelessly. The IE-WL-AP-BR-CL-ABG is rated to operate at temperatures ranging from 0 to 60°C for standard models and -40 to 75°C for wide temperature models, and is rugged enough for any harsh industrial environment.

The following topics are covered in this chapter:

- **Overview**
- **Package Checklist**
- **Product Features**
- **Product Specifications**
- **Functional Design**
  - LED Indicators
  - Beeper
  - Reset Button
  - Relay (Digital Output)

Overview

The IE-WL-AP-BR-CL-ABG (Access-Point/Bridge/Client) is ideal for applications that are hard to wire, too expensive to wire, or use mobile equipment that connects to a TCP/IP network. The IE-WL-AP-BR-CL-ABG can operate at temperatures ranging from 0 to 60°C for standard models and -40 to 75°C for extended temperature models, and is rugged enough for any harsh industrial environment. Installation is easy, with either DIN-Rail mounting or wall mounting in distribution boxes. The DIN-Rail/wall mounting capability, wide operating temperature range, and IP30 housing with LED indicators make the IE-WL-AP-BR-CL-ABG a convenient yet reliable solution for any industrial wireless application.

Package Checklist

Weidmüller's IE-WL-AP-BR-CL-ABG is shipped with the following items. If any of these items is missing or damaged, please contact your customer service representative for assistance.

- 1 IE-WL-AP-BR-CL-ABG
- Swivel-type antennas (2dBi, RP-SMA, 2.4&5GHz)
- Quick Installation Guide
- Cable holder with 1 screw
- Protective caps

Product Features

- IEEE802.11a/b/g compliant
- Three-in-one design (AP/Bridge/Client)
- Advanced wireless security:
  - 64-bit and 128-bit WEP/WPA/WPA2
  - SSID Hiding/IEEE 802.1X/RADIUS
  - Packet access control & filtering
- STP/RSTP support for network system redundancy
- Long-distance transmission support
- Turbo Roaming enables rapid handover (Client mode)
- EBR-MODULE RS232 (backup and restore module) for configuration import/export
- RS-232 console management
- 2DI+1DO for on-site monitoring and warnings
- Wide -40 to 75°C operating temperature range (-T model)
- Redundant 24 VDC power inputs or IEEE802.3af Power over Ethernet
- DIN-Rail or wall mounting
- IP30 protected high-strength metal housing

Product Specifications

WLAN Interface

Standards:

IEEE 802.11a/b/g/h for Wireless LAN

IEEE 802.11i for Wireless Security

IEEE 802.3u for 10/100BaseT(X)

IEEE 802.3af for Power-over-Ethernet

IEEE 802.1D for Spanning Tree Protocol

IEEE 802.1w for Rapid STP

IEEE 802.1Q VLAN

Spread Spectrum and Modulation (typical):

• DSSS with DBPSK, DQPSK, CCK

• OFDM with BPSK, QPSK, 16QAM, 64QAM

• 802.11b: CCK @ 11/5.5 Mbps, DQPSK @ 2 Mbps, DBPSK @ 11 Mbps

• 802.11a/g: 64QAM @ 54/48 Mbps, 16QAM @ 36/24 Mbps, QPSK @ 18/12 Mbps, BPSK @ 9/6 Mbps

Operating Channels (central frequency):

US:

2.412 to 2.462 GHz (11 channels)

5.18 to 5.24 GHz (4 channels)

EU:

2.412 to 2.472 GHz (13 channels)

5.18 to 5.24 GHz (4 channels)

Security:

• SSID broadcast enable/disable

• Firewall for MAC/IP/Protocol/Port-based filtering

• 64-bit and 128-bit WEP encryption, WPA /WPA2-Personal and Enterprise (IEEE 802.1X/RADIUS, TKIP and AES)

Transmission Rates:

802.11b: 1, 2, 5.5, 11 Mbps

802.11a/g: 6, 9, 12, 18, 24, 36, 48, 54 Mbps

TX Transmit Power:

802.11b:

Typ. 23±1.5 dBm @ 1 to 11 Mbps

802.11g:

Typ. 20±1.5 dBm @ 6 to 24 Mbps, Typ. 19±1.5 dBm @ 36 Mbps, Typ. 18±1.5 dBm @ 48 Mbps, Typ. 17±1.5 dBm @ 54 Mbps

802.11a:

Typ. 18±1.5 dBm @ 6 to 24 Mbps, Typ. 16±1.5 dBm @ 36 to 48 Mbps, Typ. 15±1.5 dBm @ 54 Mbps

RX Sensitivity:

802.11b:

-97 dBm @ 1 Mbps, -94 dBm @ 2 Mbps, -92 dBm @ 5.5 Mbps, -90 dBm @ 11 Mbps

802.11g:

-93 dBm @ 6 Mbps, -91 dBm @ 9 Mbps, -90 dBm @ 12 Mbps, -88 dBm @ 18 Mbps, -84 dBm @ 24 Mbps, -80 dBm @ 36 Mbps, -76 dBm @ 48 Mbps, -74 dBm @ 54 Mbps

802.11a:

-90 dBm @ 6 Mbps, -89 dBm @ 9 Mbps, -89 dBm @ 12 Mbps, -85 dBm @ 18 Mbps, -83 dBm @ 24 Mbps, -79 dBm @ 36 Mbps, -75 dBm @ 48 Mbps, -74 dBm @ 54 Mbps

Protocol Support

General Protocols: Proxy ARP, DNS, HTTP, HTTPS, IP, ICMP, SNTP, TCP, UDP, RADIUS, SNMP, PPPoE, DHCP

AP-only Protocols: ARP, BOOTP, DHCP, dynamic VLAN-Tags for 802.1X-Clients, STP/RSTP (IEEE 802.1D/w)

Interface

Default Antenna: 2 dBi dual-band omni-directional antenna, RP-SMA (male)
Connector for External Antennas: RP-SMA (female)
LAN Ports: 1, 10/100BaseT(X), auto negotiation speed (RJ45-type)
Console for External Antenna: RS-232 (RJ45-type)
LED Indicators: PWR1, PWR2, PoE, FAULT, STATE, signal strength, CLIENT MODE, BRIDGE MODE, WLAN, 10M, 100M
Alarm Contact: 1 relay output with current carrying capacity of 1 A @ 24 VDC
Digital Inputs: 2 electrically isolated inputs

- +13 to +30 V for state “1”
- +3 to -30 V for state “0”
- Max. input current: 8 mA

Physical Characteristics

Housing: Metal, providing IP30 protection
Weight: 850 g
Dimensions: 53.6 x 135 x 105 mm (2.11 x 5.31 x 4.13 in)
Installation: DIN-Rail mounting, wall mounting (with optional kit)

Environmental Limits

Operating Temperature:
Standard Models: 0 to 60°C (32 to 140°F)
Wide Temp. Models: -40 to 75°C (-40 to 167°F)
Storage Temperature: -40 to 85°C (-40 to 185°F)
Ambient Relative Humidity: 5% to 95% (non-condensing)

Power Requirements

Input Voltage: 12 to 48 VDC, redundant dual DC power inputs or 48 VDC Power-over-Ethernet (IEEE 802.3af compliant)
Connector: 10-pin removable terminal block
Power Consumption:

- 0.121 to 0.494 A @ 12 to 48 VDC
- 0.3 A @ 24 VDC

Reverse Polarity Protection: Present

Regulatory Approvals

Safety: EN60950-1, UL60950-1
Radio: EN300 328, EN301 893
EMC: EN301 489-1/-17, FCC Part 15, EN55022/55024, IEC61000-6-2/-4
Hazardous Location: UL/cUL Class I, Div. 2; ATEX Class I, Zone 2

Warranty

Warranty Period: 5 years

ATTENTION

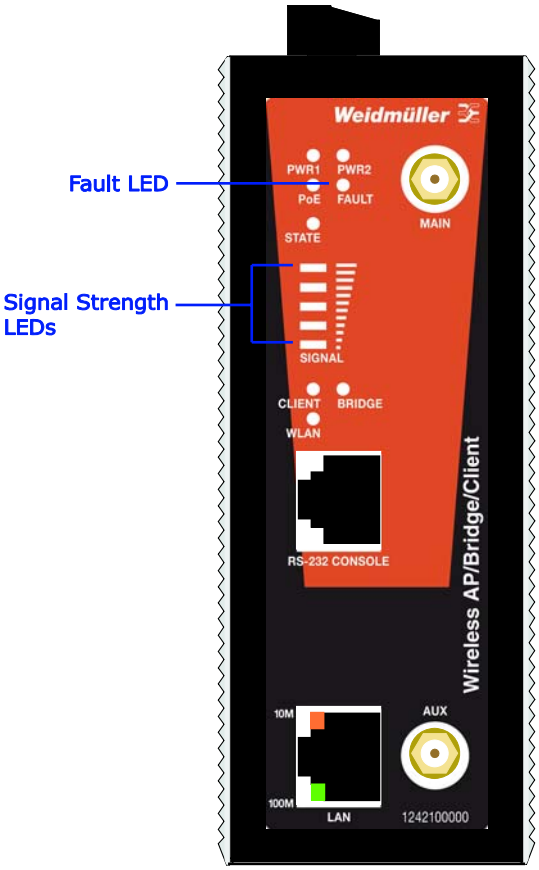
- The IE-WL-AP-BR-CL-ABG is NOT a portable mobile device and should be located at least 20 cm away from the human body.
- The IE-WL-AP-BR-CL-ABG is NOT designed for the general public. A well-trained technician should be enlisted to ensure safe deployment of IE-WL-AP-BR-CL-ABG units, and to establish a wireless network.

Functional Design

LED Indicators

The LEDs on the front panel of the IE-WL-AP-BR-CL-ABG provide a quick and easy means of determining the current operational status and wireless settings.

The **FAULT** LED indicates system failures and user-configured events. If the IE-WL-AP-BR-CL-ABG cannot retrieve the IP address from a DHCP server, the **FAULT** LED will blink at one second intervals. The **SIGNAL** LEDs indicate signal strength, and only operate in **Client** mode.



The following table summarizes how to read the device's wireless settings from the LED displays. More information is available in Chapter 3 in the "Basic Wireless Settings" section.

Basic Wireless Settings		LEDs			Note
Operation mode	**WDS**	**CLIENT**	**BRIDGE**	**SIGNAL**	
AP	Disabled	off	off	–	AP mode
AP	Enabled	off	on	–	Bridge mode: WDS is enabled
Client	–	on	off	0	Client mode: no association
Client	–	on	off	1	Client mode: associated, poor signal
Client	–	on	off	2-5	Client mode: associated, good signal

ATTENTION

The **FAULT**, **SIGNAL**, **CLIENT**, **BRIDGE**, and **WLAN** LEDs lighting up simultaneously and blinking at one-second intervals indicates that the system has failed to boot. This may be due to improper operation or an uncontrollable factor, such as an unexpected shutdown during firmware update. Instructions on how to recover the firmware can be found in Chapter 6 in the "Firmware Recovery" section.

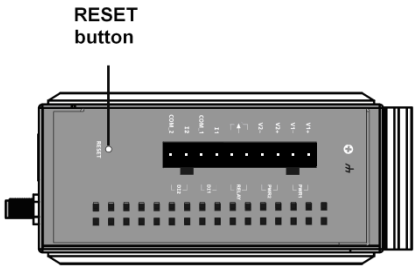
Beeper

The beeper emits two short beeps when the system is ready.

Reset Button

The **RESET** button is located on the top panel of the IE-WL-AP-BR-CL-ABG. You can reboot the IE-WL-AP-BR-CL-ABG or reset it to factory default settings by pressing the **RESET** button with a pointed object such as an unfolded paper clip.

- **System reboot:** Hold the RESET button down for under 5 seconds and then release.
- **Reset to factory default:** Hold the RESET button down for *over* 5 seconds until the **STATE** LED starts blinking green. Release the button to reset the IE-WL-AP-BR-CL-ABG.



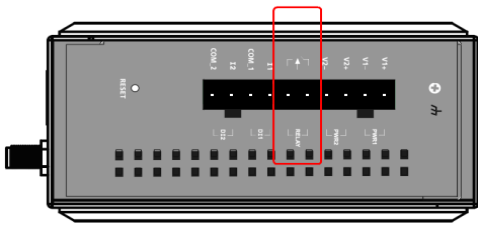
Relay (Digital Output)

The IE-WL-AP-BR-CL-ABG has one relay output consisting of the 2 terminal block contacts on the top panel, as shown below. These relay contacts are used to forward system failures and user-configured events.

The two wires attached to the relay contacts form an open circuit when a user-configured event is triggered. If a user-configured event does not occur, the relay circuit will remain closed. For safety reasons, the relay circuit is kept open when the IE-WL-AP-BR-CL-ABG is not powered up.

Summary of the IE-WL-AP-BR-CL-ABG's Relay Status

Power Status	Event	Relay
Off	–	Open
On	Yes	Open
	No	Short



2

Getting Started

This chapter explains how to install Weidmüller's IE-WL-AP-BR-CL-ABG for the first time, and quickly set up your wireless network and test whether the connection is running well. The function guide provides a convenient means of determining which functions you need to use.

The following topics are covered in this chapter:

- **First-time Installation and Configuration**
- **Communication Testing**
- **Function Map**

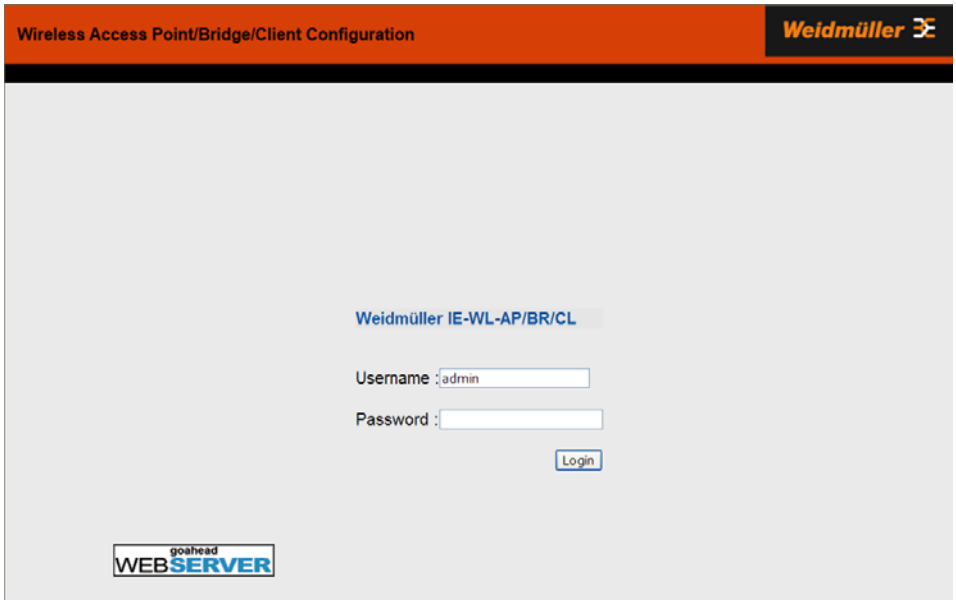
First-time Installation and Configuration

Before installing the IE-WL-AP-BR-CL-ABG, make sure that all items in the Package Checklist are in the box. You will need access to a notebook computer or PC equipped with an Ethernet port. The IE-WL-AP-BR-CL-ABG has a default IP address that must be used when connecting to the device for the first time.

- **Step 1: Select the power source.**
  The IE-WL-AP-BR-CL-ABG can be powered by a DC power input or PoE (Power over Ethernet). The IE-WL-AP-BR-CL-ABG will use whichever power source you choose.
- **Step 2: Connect the** IE-WL-AP-BR-CL-ABG **to a notebook or PC.**
  Since the IE-WL-AP-BR-CL-ABG supports MDI/MDI-X auto-sensing, you can use either a straight-through cable or crossover cable to connect the IE-WL-AP-BR-CL-ABG to a computer. The LED indicator on the IE-WL-AP-BR-CL-ABG's LAN port will light up when a connection is established.
- **Step 3: Set up the computer's IP address.**
  Choose an IP address on the same subnet as the IE-WL-AP-BR-CL-ABG. Since the IE-WL-AP-BR-CL-ABG's default IP address is **192.168.1.110**, and the subnet mask is **255.255.255.0**, you should set the IP address of the computer to **192.168.1.xxx**.

NOTE After you select **Maintenance → Load Factory Default** and click the **Submit** button, the IE-WL-AP-BR-CL-ABG will be reset to factory default settings and the IP address will be reset to **192.168.1.110**.

- **Step 4: Use the web-based manager to configure the** IE-WL-AP-BR-CL-ABG
  Open your computer's web browser and type **http://192.168.1.110** in the address field to access the homepage of the web-based Network Manager. Before the homepage opens, you will need to enter the user name and password as shown in the following figure. For first-time configuration, enter the default user name and password and then click on the **Login** button:



NOTE Default user name and password:

User Name: **admin**

Password: **Detmold**

For security reasons, we strongly recommend changing the default password. To do so, select **Maintenance → Password**, and then follow the on-screen instructions to change the password.

NOTE After you click **Submit** to apply changes the web page will refresh **(Updated)** will appear on the page and a blinking reminder will be shown on the upper-right corner of the web page:

To activate the changes click **Restart** and then **Save and Restart** after you change the settings. About 30 seconds are needed for the IE-WL-AP-BR-CL-ABG to complete the reboot procedure.

- **Step 5: Select the** IE-WL-AP-BR-CL-ABG **operation mode.**
  By default, the IE-WL-AP-BR-CL-ABG's operation mode is set to AP. You can change to Client mode in **Wireless Settings → Basic Wireless Settings**. Detailed information about configuring the IE-WL-AP-BR-CL-ABG's operation can be found in Chapter 3.
- **Step 6: Test communications.**
  In the following sections we describe two test methods that can be used to ensure that a network connection has been established.

Communication Testing

After installing the IE-WL-AP-BR-CL-ABG you can run a sample test to make sure the IE-WL-AP-BR-CL-ABG and wireless connection are functioning normally. Two testing methods are described below. Use the first method if you are using only one IE-WL-AP-BR-CL-ABG device, and use the second method if you are using two or more IE-WL-AP-BR-CL-ABG units.

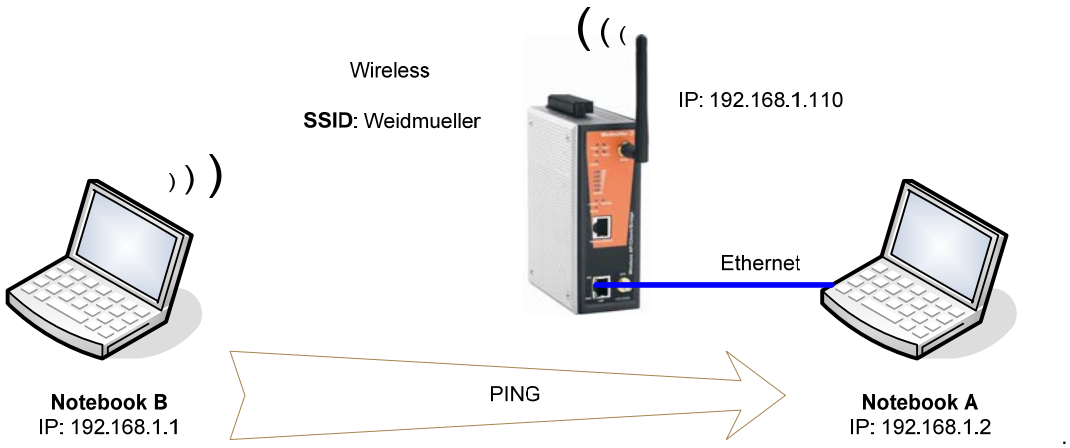
How to Test One IE-WL-AP-BR-CL-ABG

If you are only using one IE-WL-AP-BR-CL-ABG, you will need a second notebook computer equipped with a WLAN card. Configure the WLAN card to connect to the IE-WL-AP-BR-CL-ABG (NOTE: the default SSID is **Weidmueller**), and change the IP address of the second notebook (Notebook B) so that it is on the same subnet as the first notebook (Notebook A), which is connected to the IE-WL-AP-BR-CL-ABG.

After configuring the WLAN card, establish a wireless connection with the IE-WL-AP-BR-CL-ABG and open a DOS window on Notebook B. At the prompt, type

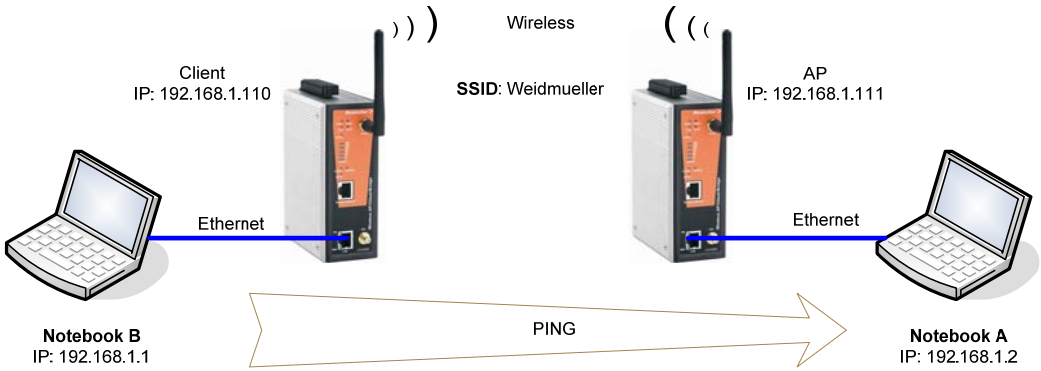
ping *<IP address of notebook A>*

and then press **Enter** (see the figure below). A "Reply from IP address …" response means the communication was successful. A "Request timed out." response means the communication failed. In this case, recheck the configuration to make sure the connections are correct.



How to Test Two or More IE-WL-AP-BR-CL-ABG Units

If you have two or more IE-WL-AP-BR-CL-ABG units, you will need a second notebook computer (Notebook B) equipped with an Ethernet port. Use the default settings for the first IE-WL-AP-BR-CL-ABG connected to notebook A and change the second or third IE-WL-AP-BR-CL-ABG connected to notebook B to Client mode, and then configure the notebooks and IE-WL-AP-BR-CL-ABG units properly.

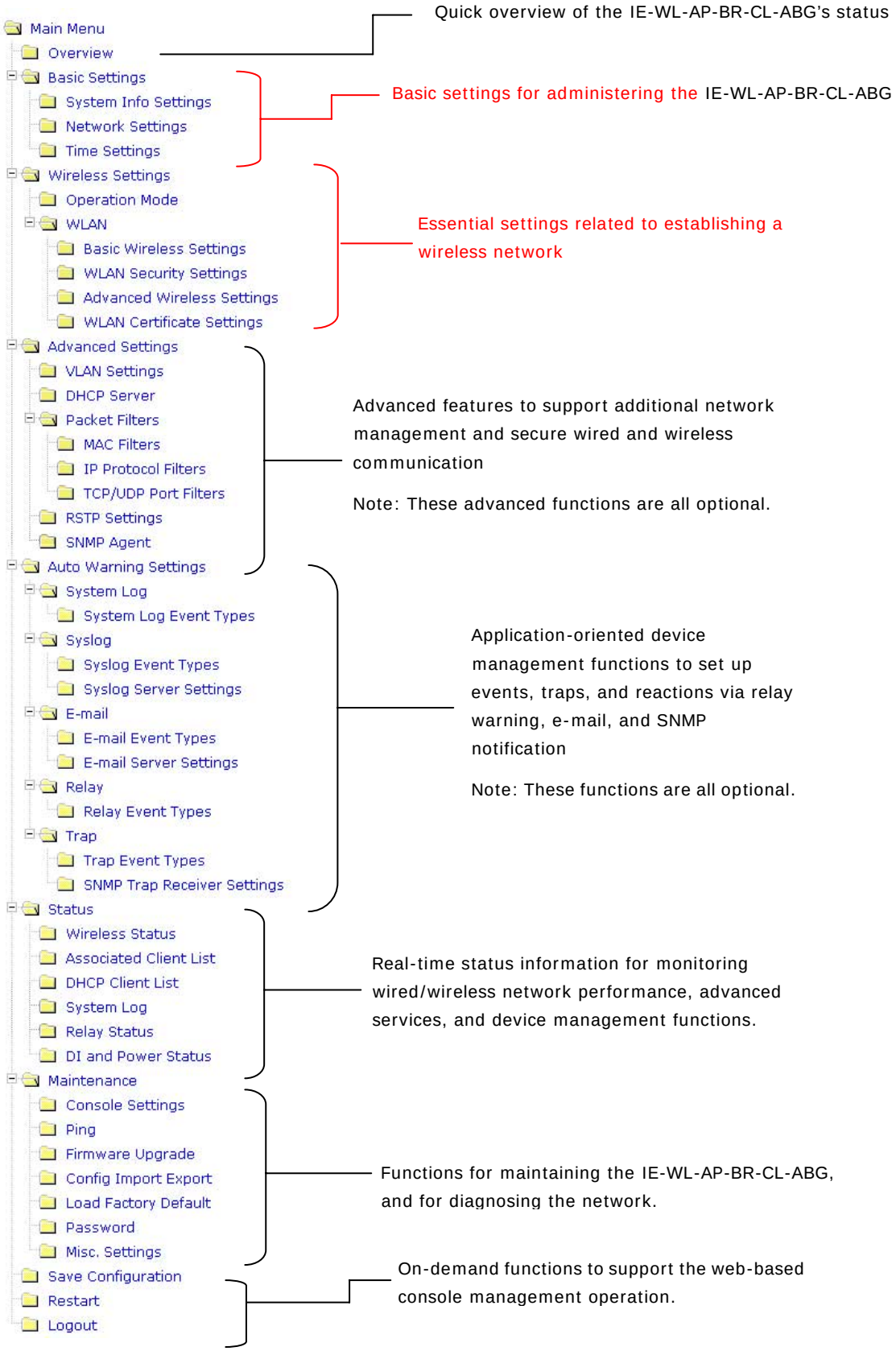


After setting up the testing environment, open a DOS window on notebook B. At the prompt, type:

ping *<IP address of notebook A>*

and then press **Enter**. A "Reply from IP address ..." response means the communication was successful. A "Request timed out" response means the communication failed. In this case, recheck the configuration to make sure the connections are correct.

Function Map



3

Web Console Configuration

In this chapter, we explain all aspects of web-based console configuration. Weidmüller's easy-to-use management functions help you set up your IE-WL-AP-BR-CL-ABG and make it easy to establish and maintain your wireless network.

The following topics are covered in this chapter:

- **Web Browser Configuration**
- **Overview**
- **Basic Settings**
  - System Info Settings
  - Network Settings
  - Time Settings
- **Wireless Settings**
- **Operation Mode**
- **Basic Wireless Settings**
  - WLAN Security Settings
  - Advanced Wireless Settings
  - WLAN Certification Settings (for EAP-TLS in Client mode only)
- **Advanced Settings**
  - Using Virtual LAN
  - Configuring Virtual LAN
  - DHCP Server (for AP mode only)
  - Packet Filters
  - RSTP Settings (for AP mode only)
  - SNMP Agent
  - Link Fault Pass-Through (for Client/Slave mode only)
- **Auto Warning Settings**
  - System Log
  - Syslog
  - E-mail
  - Relay
  - Trap
- **Status**
  - Associated Client List (for AP mode only)
  - DHCP Client List (for AP mode only)
  - System Log
  - Relay Status
  - DI and Power Status
  - Wireless Status
- **Maintenance**
  - Console Settings
  - Ping
  - Firmware Upgrade
  - Config Import Export
  - Load Factory Default
  - Password
  - Misc. Settings
- **Save Configuration**
- **Restart**
- **Logout**

Web Browser Configuration

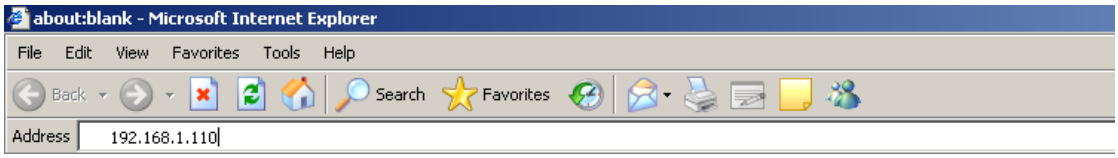
Weidmüller IE-WL-AP-BR-CL-ABG's web browser interface provides a convenient way to modify its configuration and access the built-in monitoring and network administration functions. The recommended web browser is Microsoft® Internet Explorer 7.0 or 8.0 with JVM (Java Virtual Machine) installed.

NOTE To use the IE-WL-AP-BR-CL-ABG's management and monitoring functions from a PC host connected to the same LAN as the IE-WL-AP-BR-CL-ABG, you must make sure that the PC host and the IE-WL-AP-BR-CL-ABG are on the same logical subnet. Similarly, if the IE-WL-AP-BR-CL-ABG is configured for other VLAN settings, you must make sure your PC host is on the management VLAN.

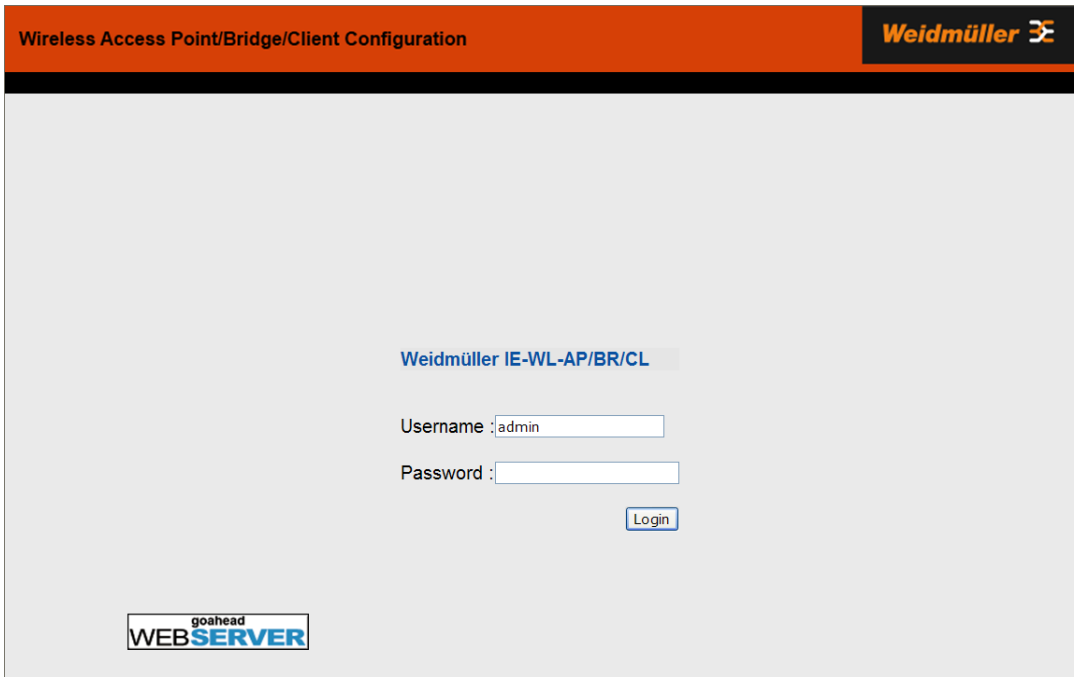
The Weidmüller IE-WL-AP-BR-CL-ABG's default IP is **192.168.1.110**.

Follow these steps to access the IE-WL-AP-BR-CL-ABG's web-based console management interface.

1. Open your web browser (e.g., Internet Explorer) and type the IE-WL-AP-BR-CL-ABG's IP address in the address field. Press **Enter** to establish the connection.

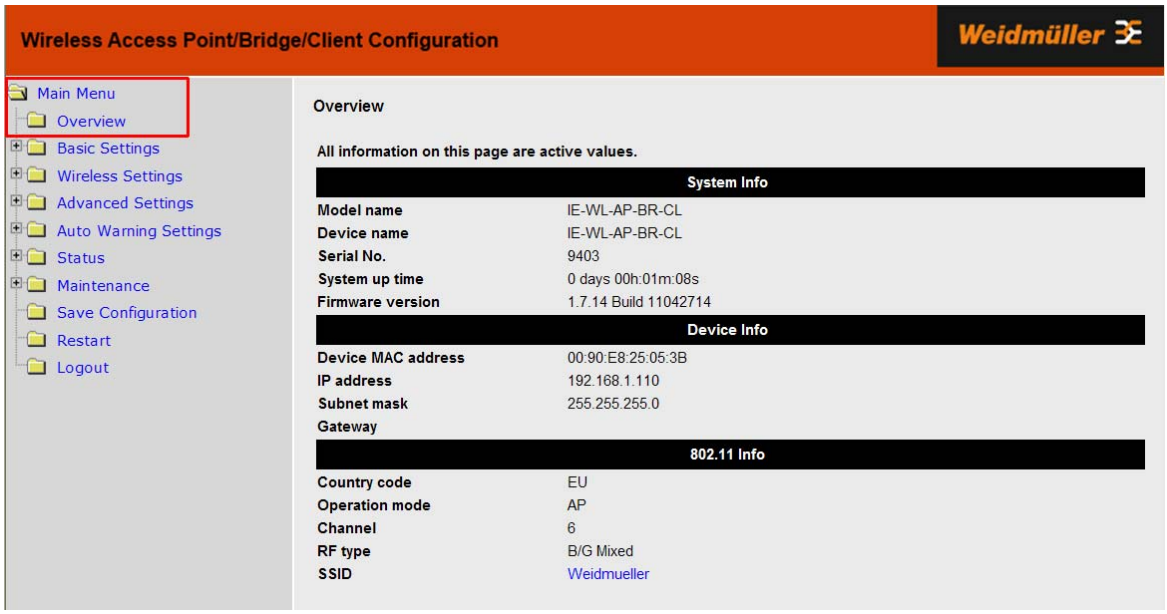

about:blank - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address 192.168.1.110

2. The Web Console Login page will open. Enter the password (default Username = **admin**; default Password = **Detmold**) and then click **Login** to continue.



3. You may need to wait a few moments for the web page to download to your computer. Note that the Model name and IP address of your IE-WL-AP-BR-CL-ABG are both shown in the title bar of the web page. This information can be used to help you identify multiple IE-WL-AP-BR-CL-ABG units.

4. Use the menu tree on the left side of the window to open the function pages to access each of the IE-WL-AP-BR-CL-ABG's functions.



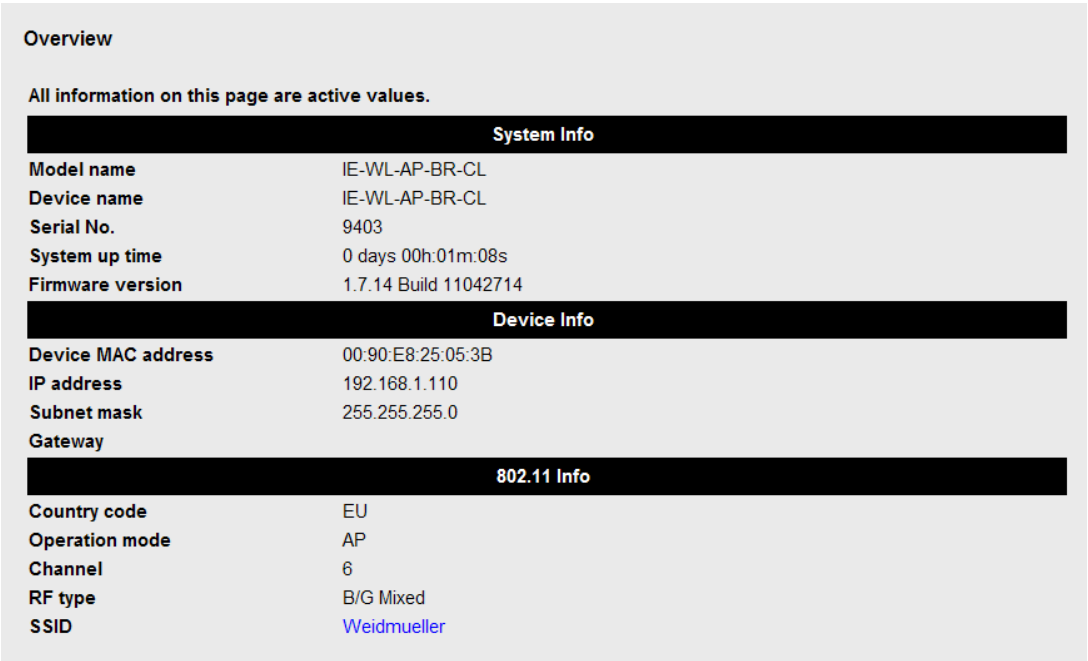
In the following paragraphs, we describe each IE-WL-AP-BR-CL-ABG management function in detail. A quick overview is available in this manual in the "Function Map" section of Chapter 2.

NOTE The model name of the IE-WL-AP-BR-CL-ABG is shown as IE-WL-AP-BR-CL-ABG-XX, where XX indicates the country code. The country code indicates the IE-WL-AP-BR-CL-ABG version and which bandwidth it uses. We use **IE-WL-AP-BR-CL-ABG-EU** as an example in the following figures. (The country code and model name that appears on your computer screen may be different than the one shown here.)

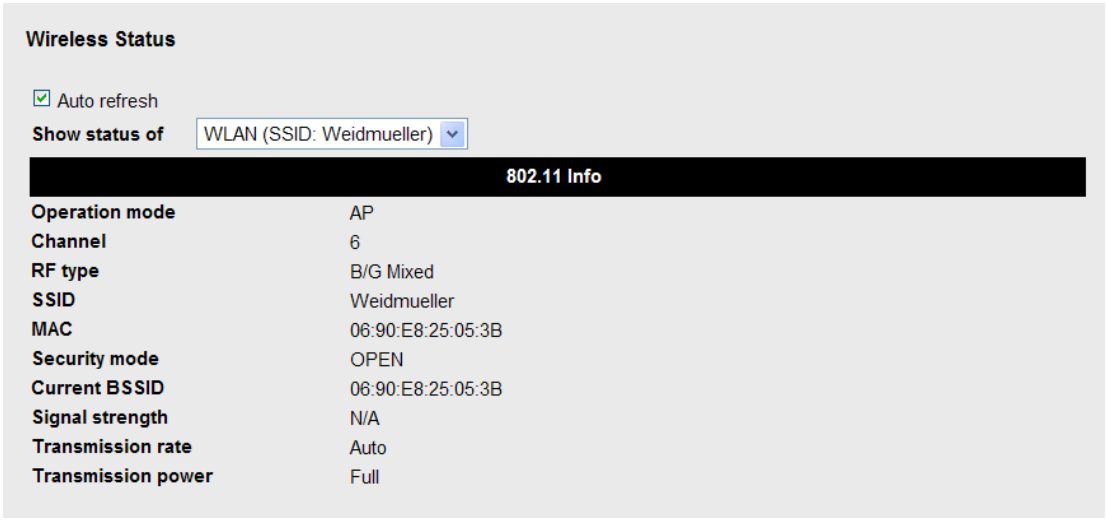
NOTE For security reasons, you will need to log back into the IE-WL-AP-BR-CL-ABG after a 5-minute time-out.

Overview

The **Overview** page summarizes the IE-WL-AP-BR-CL-ABG's current status. The information is categorized into several groups: **System info**, **Device info**, and **802.11 info**.



Click on **SSID** for more detailed 802.11 information, as shown in the following figure.



NOTE

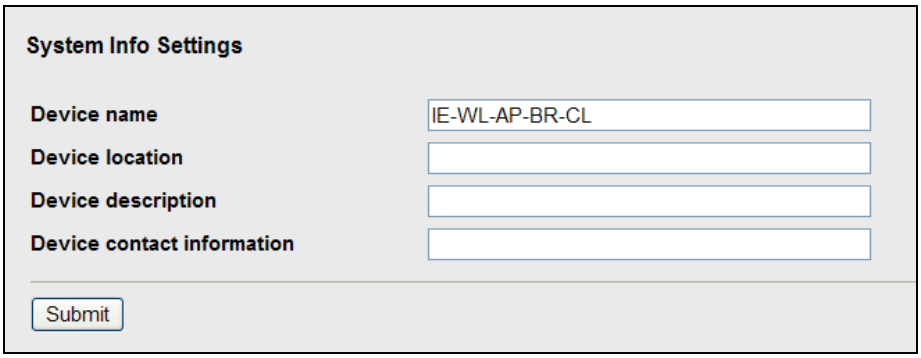
The **802.11 info** that is displayed may be different for different operation modes. For example, “Current BSSID” is not available in Client mode, and “Signal strength” is not available in AP mode.

Basic Settings

The Basic Settings group includes the most commonly used settings required by administrators to maintain and control the IE-WL-AP-BR-CL-ABG.

System Info Settings

The **System Info** items, especially ***Device name*** and ***Device description***, are displayed and included on the **Overview** page, in SNMP information, and in alarm emails. Setting **System Info** items makes it easier to identify the different IE-WL-AP-BR-CL-ABG units connected to your network.



Device name

Setting	Description	Factory Default
Max. 31 of characters	This option is useful for specifying the role or application of different IE-WL-AP-BR-CL-ABG units.	IE-WL-AP-BR-CL-ABG_<Serial No. of this IE-WL-AP-BR-CL-ABG>

Device location

Setting	Description	Factory Default
Max. of 31 characters	Specifies the location of different IE-WL-AP-BR-CL-ABG units.	None

Device description

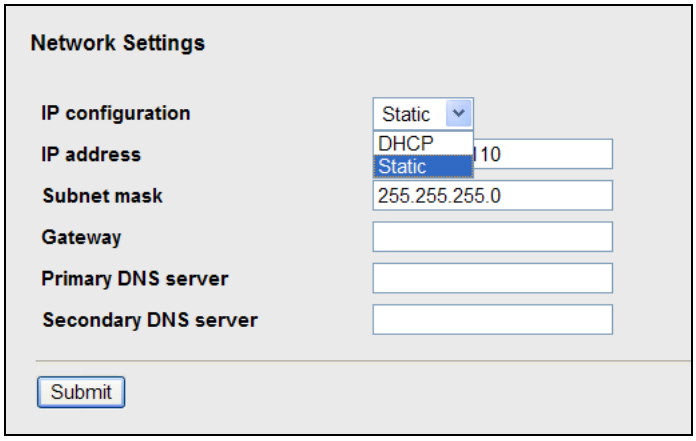
Setting	Description	Factory Default
Max. of 31 characters	Use this space to record amore detailed description of the IE-WL-AP-BR-CL-ABG	None

Device contact information

Setting	Description	Factory Default
Max. of 31 characters	Provides information about whom to contact in order to resolve problems. Use this space to record contact information of the person responsible for maintaining this IE-WL-AP-BR-CL-ABG.	None

Network Settings

The Network Settings configuration panel allows you to modify the usual TCP/IP network parameters. An explanation of each configuration item is given below.



IP configuration

Setting	Description	Factory Default
DHCP	The IE-WL-AP-BR-CL-ABG's IP address will be assigned automatically by the network's DHCP server	Static
Static	Set up the IE-WL-AP-BR-CL-ABG's IP address manually.	

IP address

Setting	Description	Factory Default
IE-WL-AP-BR-CL-ABG's IP address	Identifies the IE-WL-AP-BR-CL-ABG on a TCP/IP network.	192.168.1.110

Subnet mask

Setting	Description	Factory Default
IE-WL-AP-BR-CL-ABG's subnet mask	Identifies the type of network to which the IE-WL-AP-BR-CL-ABG is connected (e.g., 255.255.0.0 for a Class B network, or 255.255.255.0 for a Class C network).	255.255.255.0

Gateway

Setting	Description	Factory Default
IE-WL-AP-BR-CL-ABG's default gateway	The IP address of the router that connects the LAN to an outside network.	None

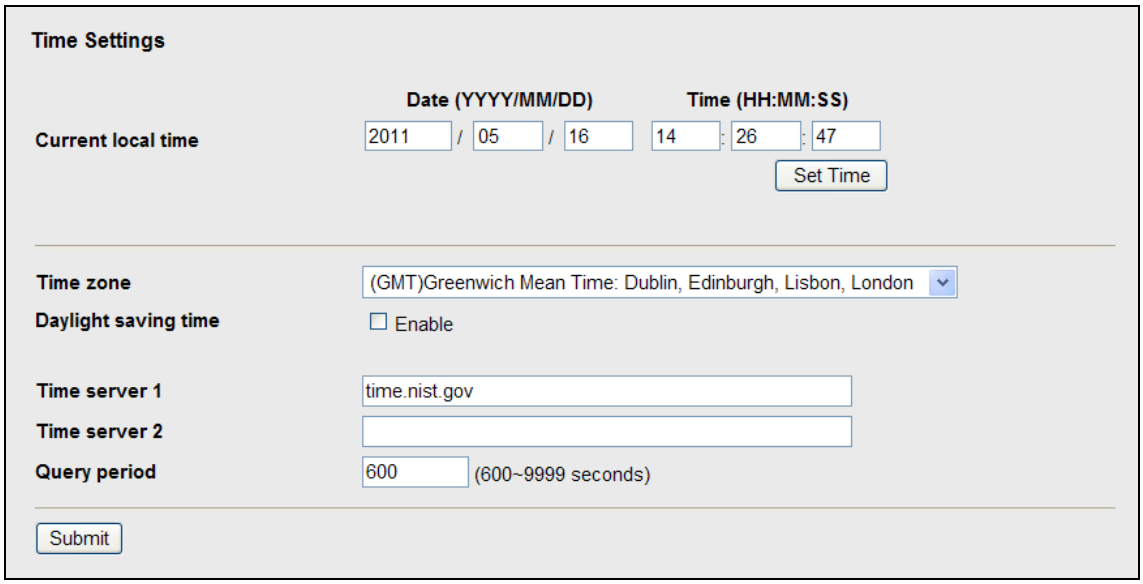
Primary / Secondary DNS server

Setting	Description	Factory Default
IP address of the	The IP address of the DNS Server used by your network. After	None

Primary/Secondary DNS server	entering the DNS Server's IP address, you can input the IE-WL-AP-BR-CL-ABG's URL (e.g., http://ap1.weidmueller.com) in your browser's address field instead of entering the IP address. The Secondary DNS server will be used if the Primary DNS server fails to connect.	

Time Settings

The IE-WL-AP-BR-CL-ABG has a time calibration function based on information from an NTP server or user specified Date and Time information. Functions such as Auto warning can add real-time information to the message.



The ***Current local time*** shows the IE-WL-AP-BR-CL-ABG's system time when you open this web page. You can click on the **Set Time** button to activate the updated date and time parameters. An "(Updated)" string will appear to indicate that the change is complete. Local time settings will be immediately activated in the system without running Save and Restart.

NOTE The IE-WL-AP-BR-CL-ABG has a built-in real time clock (RTC). We strongly recommend that users update the **Local time** for the IE-WL-AP-BR-CL-ABG after the initial setup or a long-term shutdown, especially when the network does not have an Internet connection for accessing the NTP server or there is no NTP server on the LAN.

Current local time

Setting	Description	Factory Default
User adjustable time	The date and time parameters allow configuration of the local time, with immediate activation. *Use 24-hour format: yyyy/mm/dd hh:mm:ss*	None

Time zone

Setting	Description	Factory Default
User selectable time zone	The time zone setting allows conversion from GMT (Greenwich Mean Time) to local time.	GMT (Greenwich Mean Time)

ATTENTION

Changing the time zone will automatically adjust the **Current local time**. You should configure the **Time zone** before setting the **Current local time**.

Daylight saving time

Setting	Description	Factory Default
Enable/ Disable	Daylight saving time (also know as DST or summer time) involves advancing clocks (usually 1 hour) during the summer time to provide an extra hour of daylight in the afternoon.	Disable

When **Daylight saving time** is enabled, the following parameters will be shown:

- **Starts at:** The date that daylight saving time begins.
- **Stops at:** The date that daylight saving time ends.
- **Time offset:** Indicates how many hours forward the clock should be advanced.

Time server 1/2

Setting	Description	Factory Default
IP/Name of Time Server 1/2	IP or Domain name of the NTP time server. The 2nd NTP server will be used if the 1st NTP server fails to connect.	None

Query period

Setting	Description	Factory Default
Query period time (1 to 9999 seconds)	This parameter determines how often the time is updated from the NTP server.	600 (seconds)

Wireless Settings

The essential settings for wireless networks are presented in this function group. Settings must be properly set before establishing your wireless network. Familiarize yourself with the following terms before starting the configuration process:

AP/Bridge: This mode provides both Access Point and Static LAN-to-LAN Bridging functionality. The static LAN-to-LAN bridging function is supported by the Wireless Distribution System (WDS).

AP Client: This mode is for Dynamic LAN-to-LAN Bridging or Device-to-LAN scenarios. The AP Client automatically establishes bridge links with other APs.

In either AP/Bridge or AP Client mode, the IE-WL-AP-BR-CL-ABG forwards packets between its Ethernet interface (LAN) and wireless interface (WLAN) to connect wired hosts on the Ethernet side with wireless host(s) on the wireless side. There are two types of wireless links are specified by the IEEE802.11 standard:

- **STA-AP:** This type of wireless link is established between an IEEE802.11 Station (STA) and an IEEE802.11 Access Point (AP). An STA is usually a client computer (PC or PDA) with a WLAN network interface card (NIC). The Client mode is actually an STA.
- **WDS:** This type of wireless link is established between two IEEE802.11 APs. Wireless packets transmitted along the WDS link comply with the IEEE802.11 WDS (Wireless Distribution System) format at the link layer. Refer to the “Wireless Distribution System (WDS)” section in Chapter 5 for details. Keep in mind that WPA/WPA2 **CANNOT** be supported in WDS.

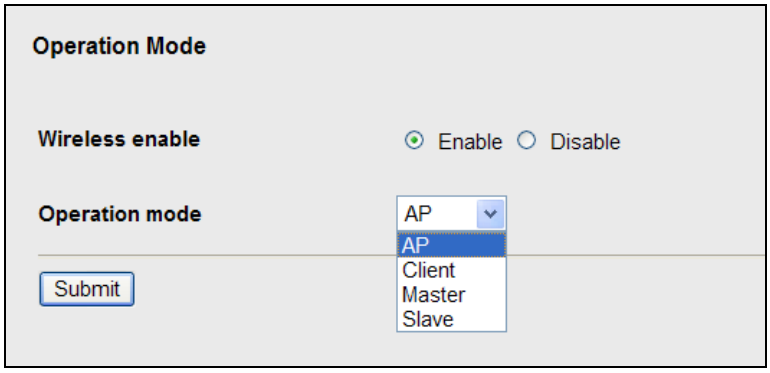
To establish a static bridge link based on the WDS, the APs at both end of the WDS link must be configured manually with each other’s MAC addresses. To establish a dynamic bridge link between an AP and a Client, both devices must be configured with the same channel, and security settings (see “WLAN Security Settings” for details). Moreover, the same SSID is also needed for clients that roam the APs in Bridge mode. The AP Client automatically scans for any AP that is using the matched SSID and establishes a bridge link with the scanned AP.

When the IE-WL-AP-BR-CL-ABG is configured for **Client** mode, it can be used as an Ethernet-to-wireless (or LAN-to-WLAN) network adapter. For example, a notebook computer equipped with an Ethernet adaptor but no wireless card can be connected to this device with an Ethernet cable to provide wireless connectivity to another AP.

NOTE Although it is more convenient to use dynamic bridging, there is a limitation—the AP Client can only transmit IP-based packets between its wireless interface (WLAN) and Ethernet interface (LAN); other types of traffic (such as IPX and AppleTalk) are not forwarded.

Operation Mode

The IE-WL-AP-BR-CL-ABG supports four main operation modes—Client, AP, Master, and Slave—each of which plays a distinct role on the wireless network.



Wireless Enable

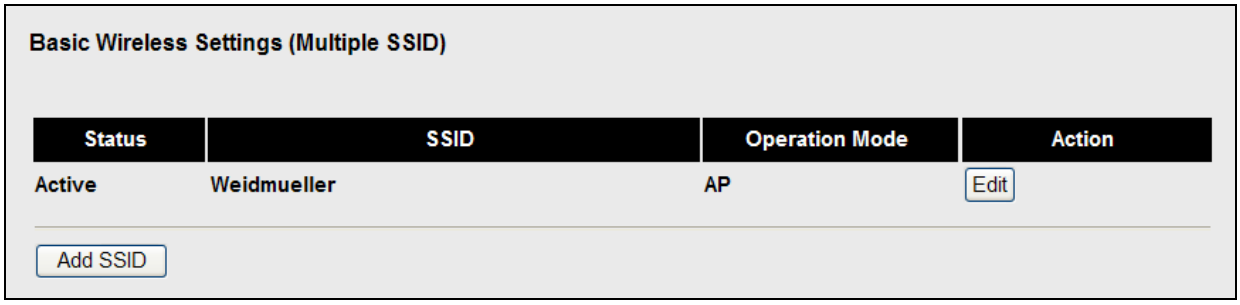
Setting	Description	Factory Default
Enable/Disable	The RF (Radio Frequency) module can be manually turned on or off. This function is available in AP operation mode only.	Enable

Operation Mode

Setting	Description	Factory Default
AP	The IE-WL-AP-BR-CL-ABG plays the role of wireless AP/Bridge.	AP
Client	The IE-WL-AP-BR-CL-ABG plays the role of wireless AP Client.	
Master	The IE-WL-AP-BR-CL-ABG plays the role of wireless Master.	
Slave	The IE-WL-AP-BR-CL-ABG plays the role of wireless Slave.	

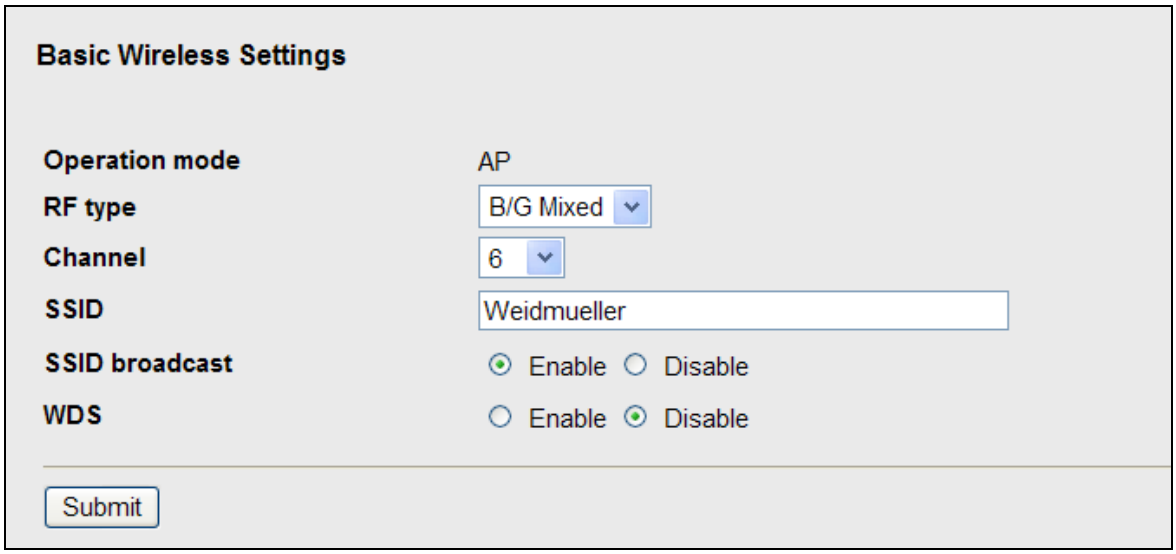
Basic Wireless Settings

The “WLAN Basic Setting Selection” panel is used to add and edit SSIDs. An SSID is a unique identifier that wireless networking devices use to establish and maintain wireless connectivity. Multiple access points on a network or sub-network can use the same SSIDs. You can configure your IE-WL-AP-BR-CL-ABG to use up to 9 SSIDs, and configure each SSID differently. All of the SSIDs are active at the same time; that is, client devices can use any of the SSIDs to associate with the access point.



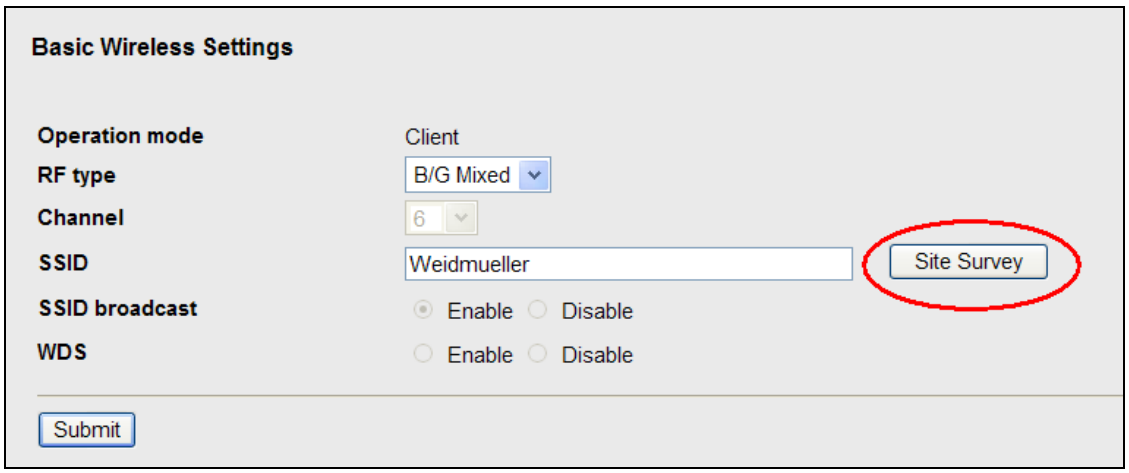
Click on **Add SSID** to create more SSIDs.

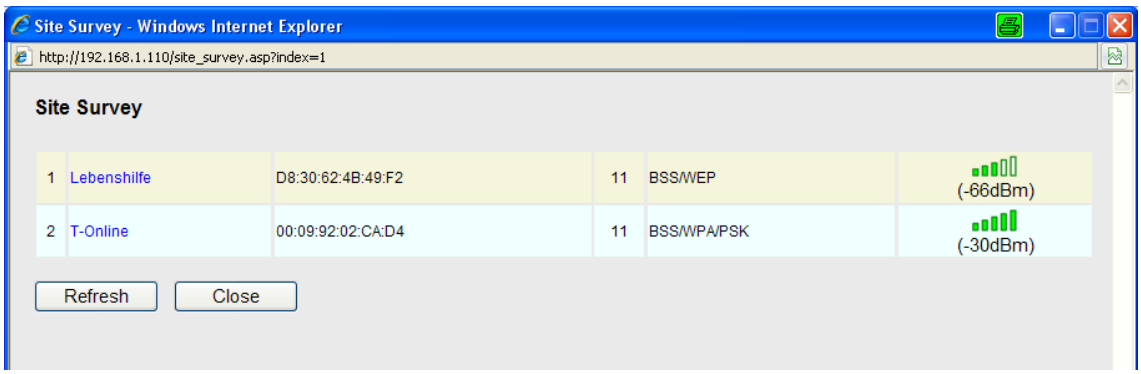
Click on **Edit** to assign different configuration settings to each SSID. The configuration panel appears as follows:



NOTE

When you switch to **Client** mode, a **Site Survey** button will be available on the Basic Wireless Settings panel. Click the "Site Survey" button to view information about available APs, as shown in the following figure. You can click on the SSID of an entity and bring the value of its SSID onto the SSID field of the Basic Wireless Settings page. Click the **Refresh** button to re-scan and update the table.





NOTE

If the **Gateway** field in **Basic Settings → Network Settings** is empty, a warning message will appear, reminding you to set the default gateway when **Client** mode is enabled. You can ignore this message if you are only planning a local network and packets will not be sent outside the network.

RF type

Setting	Description	Factory Default
A	Supports IEEE802.11a standard only	B/G Mixed
B	Supports IEEE802.11b standard only	
G	Supports IEEE802.11g standard only	
B/G Mixed	Supports both of IEEE802.11b/g standards, but 802.11g can be slowed down when 802.11b clients are on the network	

Channel (for AP/Master mode only)

Setting	Description	Factory Default
Available channels vary with RF type	IE-WL-AP-BR-CL-ABG plays a role of wireless AP.	6 (in B/G Mixed mode)

SSID

Setting	Description	Factory Default
Max. of 31 characters	The SSID of a client and the SSID of the AP must be identical for the client and AP to be able to communicate with each other.	Weidmueller

SSID broadcast (for AP/Master mode only)

Setting	Description	Factory Default
Enable/ Disable	SSID can be broadcast or not	Enable

NOTE

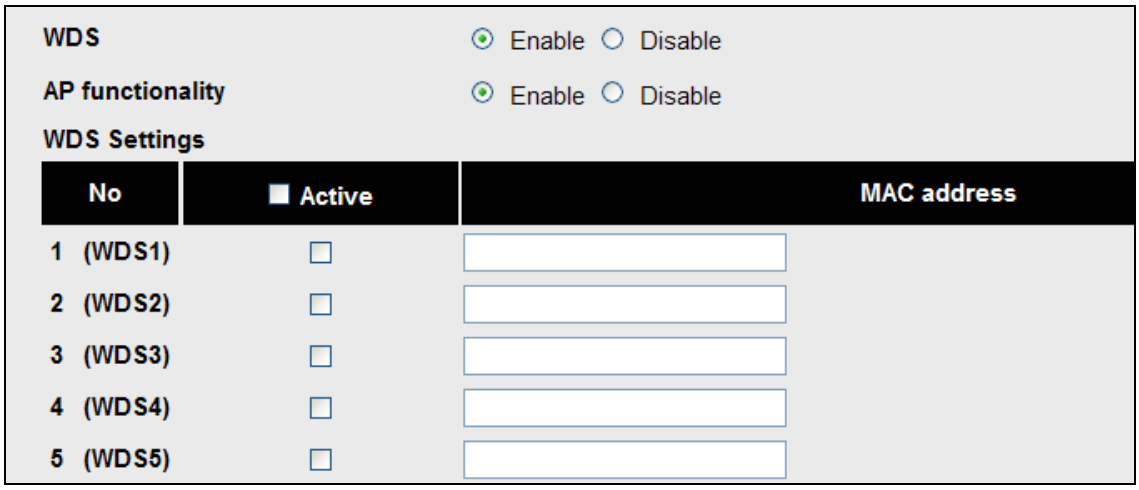
The IE-WL-AP-BR-CL-ABG-EU (for European frequency bands) only connects SSID-hidden APs in all IEEE802.11b/g channels.

WDS (for AP mode only)

Setting	Description	Factory Default
Enable/Disable	IE-WL-AP-BR-CL-ABG supports WDS or not.	Disable

NOTE

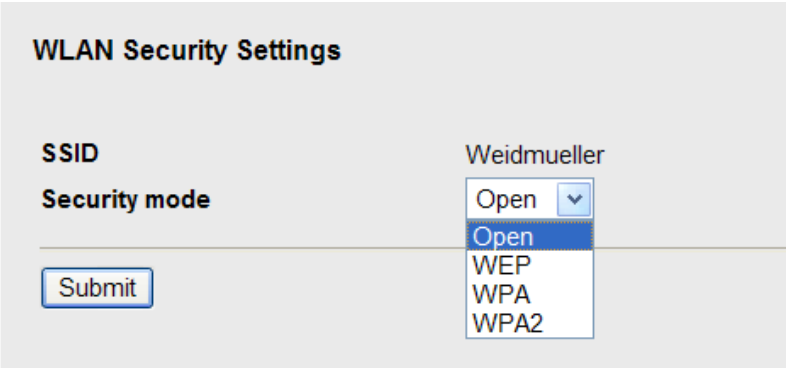
When **WDS** is enabled, you can use a pure point-to-point WDS link by disabling **AP functionality**. The IE-WL-AP-BR-CL-ABG provides 8 entities for WDS settings and can support up to 8 WDS links to other APs or wireless bridges. The list appears when WDS **Enable** is checked. Enter the MAC address to set up a WDS link. Remember to activate a WDS link by checking the **Active** check box.



WLAN Security Settings

The IE-WL-AP-BR-CL-ABG provides four standardized wireless security modes: **Open**, **WEP** (Wired Equivalent Privacy), **WPA** (Wi-Fi Protected Access), and **WPA2**. Several security modes are available in the IE-WL-AP-BR-CL-ABG by selecting ***Security mode*** and ***WPA type***:

- **Open:** No authentication, no data encryption.
- **WEP:** Static WEP (Wired Equivalent Privacy) keys must be configured manually.
- **WPA / WPA2-Personal:** Also known as WPA/WPA2-PSK. You will need to specify the Pre-Shared Key in the ***Passphrase*** field, which will be used by the TKIP or AES engine as a master key to generate keys that actually encrypt outgoing packets and decrypt incoming packets.
- **WPA / WPA2-Enterprise:** Also called WPA/WPA2-EAP (Extensible Authentication Protocol). In addition to device-based authentication, WPA/WPA2-Enterprise enables user-based authentication via IEEE802.1X. The IE-WL-AP-BR-CL-ABG can support three EAP methods: EAP-TLS, EAP-TTLS, and EAP-PEAP.



Security mode

Setting	Description	Factory Default
Open	No authentication	Open
WEP	Static WEP is used	
WPA*	WPA is used	
WPA2*	Fully supports IEEE802.11i with “TKIP/AES + 802.1X”	

**WPA and WPA2 are not supported in WDS (Bridge) mode.*

Open

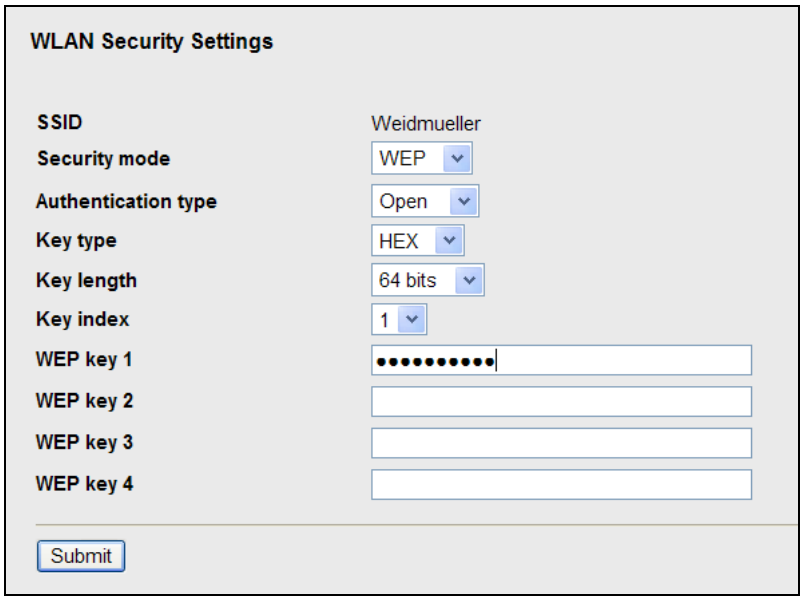
For security reasons, you should **NOT** set security mode to Open System, since authentication and data encryption are **NOT** performed in Open System mode.

WEP

According to the IEEE802.11 standard, WEP can be used for authentication and data encryption to maintain confidentiality. **Shared** (or **Shared Key**) authentication type is used if WEP authentication and data encryption are both needed. Normally, **Open** (or **Open System**) authentication type is used when WEP data encryption is run with authentication.

When WEP is enabled as a security mode, the length of a key (so-called WEP seed) can be specified as 64/128 bits, which is actually a 40/104-bit secret key with a 24-bit initialization vector. The IE-WL-AP-BR-CL-ABG provides 4 entities of WEP key settings that can be selected to use with ***Key index***. The selected key setting specifies the key to be used as a *send-key* for encrypting traffic from the AP side to the wireless client side. All 4 WEP keys are used as *receive-keys* to decrypt traffic from the wireless client side to the AP side.

The WEP key can be presented in two ***Key types***, HEX and ASCII. Each ASCII character has 8 bits, so a 40-bit (or 64-bit) WEP key contains 5 characters, and a 104-bit (or 128-bit) key has 13 characters. In hex, each character uses 4 bits, so a 40-bit key has 10 hex characters, and a 128-bit key has 26 characters.



Authentication type

Setting	Description	Factory Default
Open	Data encryption is enabled, but without authentication	Open
Shared	Data encryption and authentication are both enabled.	

Key type

Setting	Description	Factory Default
HEX	Specifies WEP keys in hex-decimal number form	HEX
ASCII	Specifies WEP keys in ASCII form	

Key length

Setting	Description	Factory Default
64 bits	Uses 40-bit secret keys with 24-bit initialization vector	64 bits
128 bits	Uses 104-bit secret key with 24-bit initialization vector	

Key index

Setting	Description	Factory Default
1-4	Specifies which WEP key is used	Open

WEP key 1-4

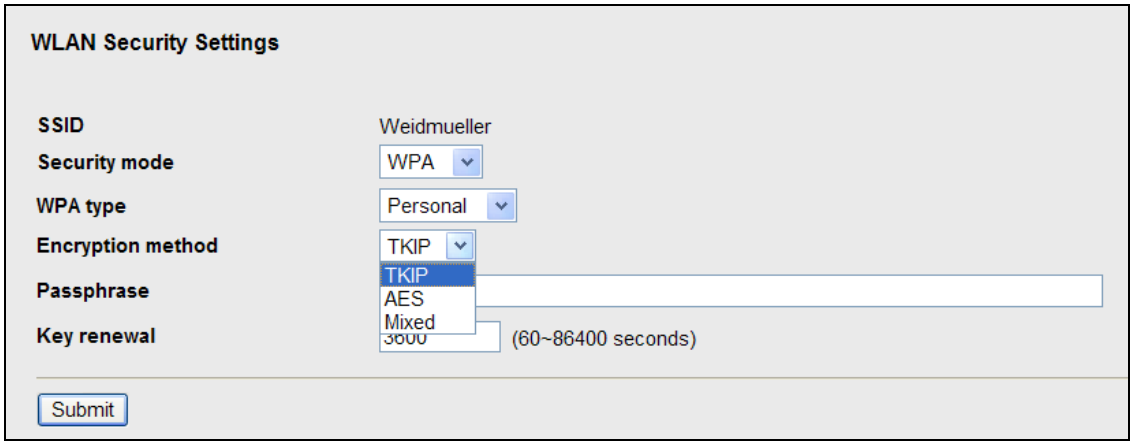
Setting	Description	Factory Default
ASCII type: 64 bits: 5 chars 128 bits: 13chars HEX type: 64 bits: 10 hex chars 128 bits: 26 hex chars	A string that can be used as a WEP seed for the RC4 encryption engine.	None

WPA / WPA2-Personal

WPA (Wi-Fi Protected Access) and WPA2 represent significant improvements over the WEP encryption method. WPA is a security standard based on 802.11i draft 3, while WPA2 is based on the fully ratified version of 802.11i. The initial vector is transmitted, encrypted, and enhanced with its 48 bits, twice as long as WEP. The key is regularly changed so that true session is secured.

Even though AES encryption is only included in the WPA2 standard, it is widely available in the WPA security mode of some wireless APs and clients as well. The IE-WL-AP-BR-CL-ABG also supports AES algorithms in WPA and WPA2 for better compatibility.

Personal versions of WPA/WPA2, also known as WPA/WPA-PSK (*Pre-Shared Key*), provide a simple way of encrypting a wireless connection for high confidentiality. A ***Passphrase*** is used as a basis for encryption methods (or cipher types) in a WLAN connection. The passphrases should be complicated and as long as possible. There must be at least 8of ASCII characters in the Passphrase, and it could go up to 63. For security reasons, this passphrase should only be disclosed to users who need it, and it should be changed regularly.



WPA type

Setting	Description	Factory Default
Personal	Provides Pre-Shared Key-enabled WPA and WPA2	Personal
Enterprise	Provides enterprise-level security for WPA and WPA2	

Encryption method

Setting	Description	Factory Default
TKIP	Temporal Key Integrity Protocol is enabled	TKIP
AES	Advance Encryption System is enabled	
Mixed*	Provides TKIP broadcast key and TKIP+AES unicast key for some legacy AP clients. This option is rarely used.	

**This option is available in AP/Master mode only, and does not support AES-enabled clients.*

Passphrase

Setting	Description	Factory Default
8 to 63 characters	Master key to generate keys for encryption and decryption	None

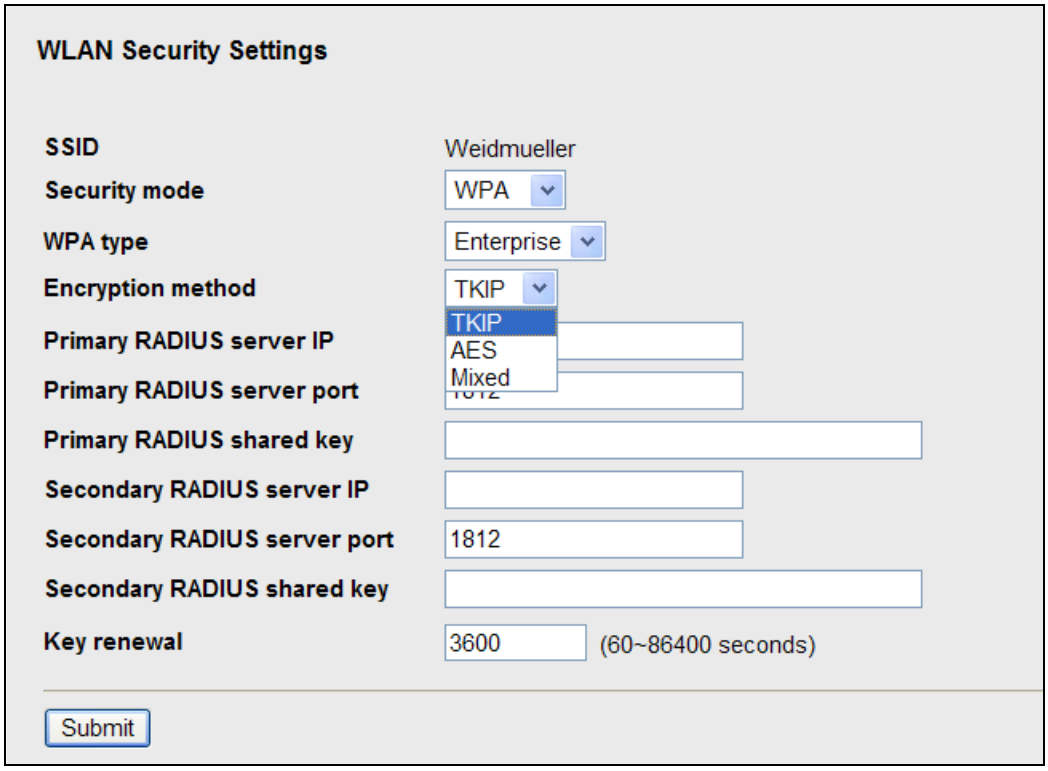
Key renewal (for AP/Master mode only)

Setting	Description	Factory Default
60 to 86400 seconds (1 minute to 1 day)	Specifies the time period of group key renewal	3600 (seconds)

NOTE The ***key renewal*** value dictates how often the wireless AP encryption keys should be changed. The security level is generally higher if you set the key renewal value to a shorter number, which forces the encryption keys to be changed more frequently. The default value is 3600 seconds (60 minutes). Longer time periods can be considered if the line is not very busy.

WPA/WPA2-Enterprise (for AP/Master mode)

By setting ***WPA type*** to **Enterprise**, you can use **EAP** (*Extensible Authentication Protocol*), a framework authentication protocol used by 802.1X to provide network authentication. In these Enterprise-level security modes, a back-end RADIUS (Remote Authentication Dial-In User Service) server is needed if IEEE 802.1X functionality is enabled in WPA /WPA2. The IEEE 802.1X protocol also offers the possibility of carrying out an efficient connection authentication on a large-scale network. It is not necessary to exchange keys or passphrases.



WPA type

Setting	Description	Factory Default
Personal	Provides Pre-Shared Key-enabled WPA and WPA2	Personal
Enterprise	Provides enterprise-level security for WPA and WPA2	

Encryption method

Setting	Description	Factory Default
TKIP	Temporal Key Integrity Protocol is enabled	TKIP
AES	Advance Encryption System is enabled	
Mixed*	Provides TKIP broadcast key and TKIP+AES unicast key for some legacy AP clients. This option is rarely used.	

**This option is available in AP/Master mode only, and cannot support AES-enabled clients.*

Primary/Secondary RADIUS server IP

Setting	Description	Factory Default
The IP address of RADIUS server	Specifies the delegated RADIUS server for EAP	None

Primary/Secondary RADIUS port

Setting	Description	Factory Default
Port number	Specifies the port number of the delegated RADIUS server	1812

Primary/ Secondary RADIUS shared key

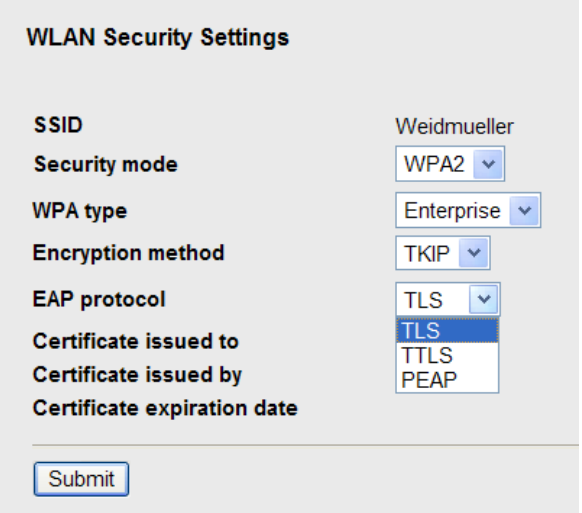
Setting	Description	Factory Default
Max. of 31 characters	The secret key shared between AP and RADIUS server	None

Key renewal

Setting	Description	Factory Default
60 to 86400 seconds (1 minute to 1 year)	Specifies the time period of group key renewal	3600 (seconds)

WPA/WPA2-Enterprise (for Client/Slave mode)

When used as a client, the IE-WL-AP-BR-CL-ABG can support three EAP methods (or ***EAP protocols***): **EAP-TLS**, **EAP-TTLS**, and **EAP-PEAP**, corresponding to WPA/WPA-Enterprise settings on the AP side.



Encryption method

Setting	Description	Factory Default
TKIP	Temporal Key Integrity Protocol is enabled	TKIP
AES	Advance Encryption System is enabled	

EAP Protocol

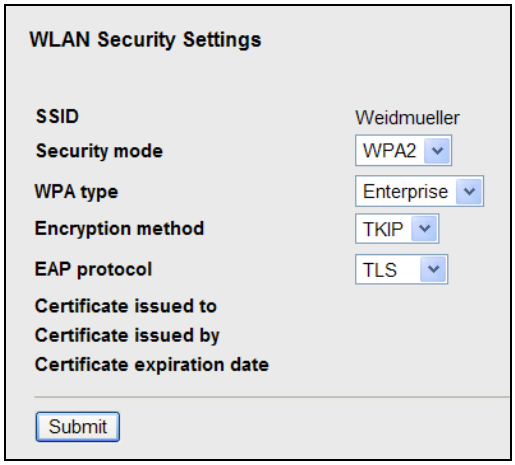
Setting	Description	Factory Default
TLS	Specifies Transport Layer Security protocol	TLS
TTLS	Specifies Tunneled Transport Layer Security	
PEAP	Specifies Protected Extensible Authentication Protocol, or Protected EAP	

Before choosing the EAP protocol for your WPA/WPA2-Enterprise settings on the client end, please contact the network administrator to make sure the system supports the protocol on the AP end. Detailed information on these three popular EAP protocols is presented in the following sections.

EAP-TLS

TLS is the standards-based successor to Secure Socket Layer (SSL). It can establish a trusted communication channel over a distrusted network. TLS provides mutual authentication through certificate exchange. EAP-TLS is also secure to use. You are required to submit a digital certificate to the authentication server for validation, but the authentication server must also supply a certificate.

You can use **Basic Wireless Settings → WLAN Certificate Settings** to import your WLAN certificate and enable EAP-TLS on the client end.



You can check the current certificate status in ***Current Status*** if it is available.

- **Certificate issued to:** Shows the certificate user
- **Certificate issued by**: Shows the certificate issuer
- **Certificate expiration date**: Indicates when the certificate has expired

EAP-TTLS

It is usually much easier to re-use existing authentication systems, such as a Windows domain or Active Directory, LDAP directory, or Kerberos realm, rather than creating a parallel authentication system. As a result, TTLS (Tunneled TLS) and PEAP (Protected EAP) are used to support the use of so-called “legacy authentication methods.”

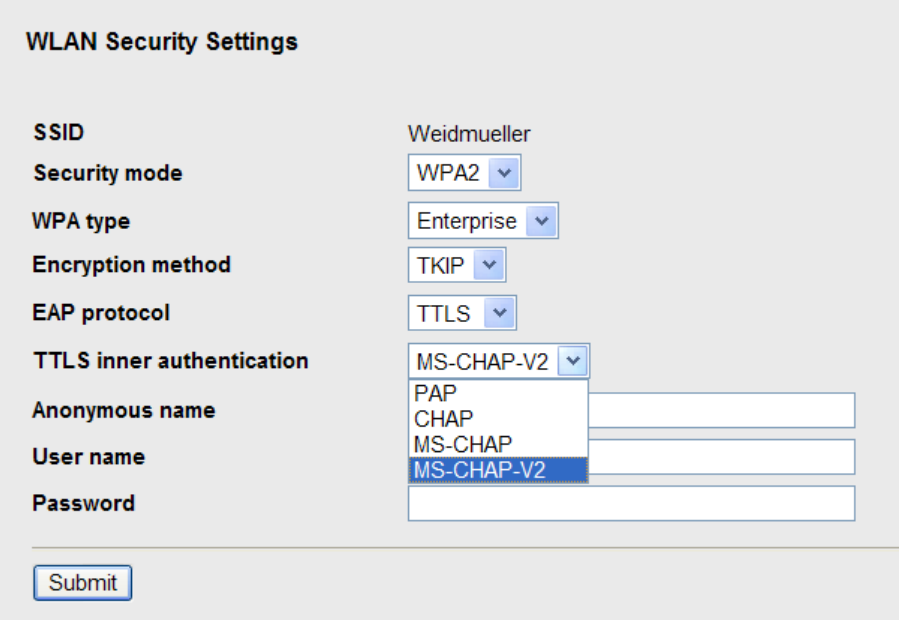
TTLS and PEAP work in a similar way. First, they establish a TLS tunnel (EAP-TLS for example), and validate whether the network is trustworthy with digital certificates on the authentication server. This step establishes a tunnel that protects the next step (or “inner” authentication), and consequently is sometimes referred to as “outer” authentication. The TLS tunnel is then used to encrypt an older authentication protocol that authenticates the user for the network.

As you can see, digital certificates are still needed for outer authentication in a simplified form. Only a small number of certificates are required, which can be generated by a small certificate authority. Certificate reduction makes TTLS and PEAP much more popular than EAP-TLS.

The IE-WL-AP-BR-CL-ABG provides some non-cryptographic EAP methods, including **PAP**, **CHAP**, **MS-CHAP**, and **MS-CHAP-V2**. These EAP methods are not recommended for direct use on wireless networks. However, they may be useful as inner authentication methods with TTLS and PEAP.

Because the inner and outer authentications can use distinct user names in TTLS and PEAP, you can use an anonymous user name for the outer authentication, with the true user name only shown through the encrypted channel. Keep in mind that not all client software supports anonymous alteration. Confirm this with the network

administrator before you enable identity hiding in TTLS and PEAP.



TTL Inner Authentication

Setting	Description	Factory Default
PAP	Password Authentication Protocol is used	MS-CHAP-V2
CHAP	Challenge Handshake Authentication Protocol is used	
MS-CHAP	Microsoft CHAP is used	
MS-CHAP-V2	Microsoft CHAP version 2 is used	

Anonymous

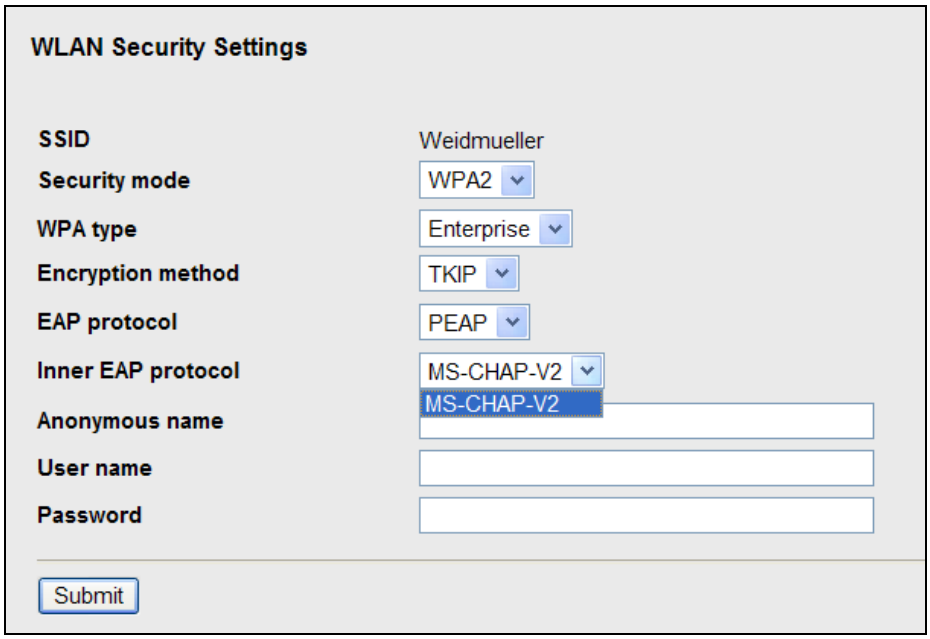
Setting	Description	Factory Default
Max. of 31 characters	A distinct name used for outer authentication	None

User name & Password

Setting	Description	Factory Default
	User name and password used in inner authentication	None

PEAP

There are a few differences in the TTLS and PEAP inner authentication procedures. TTLS uses the encrypted channel to exchange attribute-value pairs (AVPs), while PEAP uses the encrypted channel to start a second EAP exchange inside of the tunnel. The IE-WL-AP-BR-CL-ABG provides **MS-CHAP-V2** merely as an EAP method for inner authentication.



Inner EAP protocol

Setting	Description	Factory Default
MS-CHAP-V2	Microsoft CHAP version 2 is used	MS-CHAP-V2

Anonymous

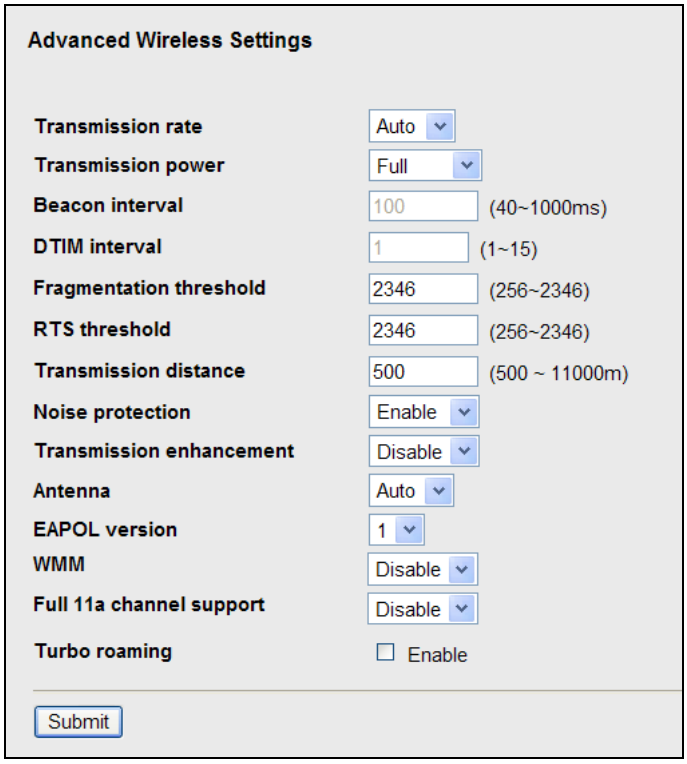
Setting	Description	Factory Default
Max. of 31 characters	A distinct name used for outer authentication	None

User name & Password

Setting	Description	Factory Default
	User name and password used in inner authentication	None

Advanced Wireless Settings

Additional wireless-related parameters are presented in this section to help you set up your wireless network in detail.



Transmission Rate

Setting	Description	Factory Default
Auto	The IE-WL-AP-BR-CL-ABG senses and adjusts the data rate automatically	Auto
Available rates	Users can manually select a target transmission data rate	

Transmission Power

Setting	Description	Factory Default
Auto	Specifies wireless signal coverage by automatically selecting the strength of Tx power	Full
Full	Equivalent to full Tx power	
High	-5 dB of maximum full Tx power	
Medium	-10 dB of maximum full Tx power	
Low	-15 dB of maximum full Tx power	

NOTE **Tx power at "Full"**
- US model: 17 dB
- EU model: 16 dB

RF type = A (Channel 36 ~ 48)

Setting	Description	Factory Default
Auto	Specifies wireless signal coverage by automatically selecting the strength of Tx power	Full
Full	Equivalent to full Tx power	
High	-4 dB of full Tx power	
Medium	-8 dB of full Tx power	
Low	-12 dB of full Tx power	

NOTE **Tx power at "Full"**
- US model: 14 dB
- EU model: 16 dB

Beacon Interval (for AP/Master mode only)

Setting	Description	Factory Default
Beacon Interval (40 to 1000 ms)	Indicates the frequency interval of the beacon	100 (ms)

DTIM Interval (for AP/Master mode only)

Setting	Description	Factory Default
Data Beacon Rate (1 to 15)	Indicates how often the IE-WL-AP-BR-CL-ABG sends out a Delivery Traffic Indication Message	1

Fragmentation threshold

Setting	Description	Factory Default
Fragment Length (256 to 2346)	Specifies the maximum size a data packet before splitting and creating another new packet	2346

RTS threshold

Setting	Description	Factory Default
RTS/CTS Threshold (256 to 2346)	Determines how large a packet can be before the Access Point coordinates transmission and reception to ensure efficient communication	2346

NOTE You can refer to the related glossaries in Chapter 5 for detailed information about the above-mentioned settings. By setting these parameters properly, you can better tune the performance of your wireless network.

Transmission distance

Setting	Description	Factory Default
Distance or max. range for transmission (500 to 10000 m)	Specifies the transmission distance or max. range between two IE-WL-AP-BR-CL-ABG devices. This parameter should be set properly, especially for long-distance communication.	500

Noise protection

Setting	Description	Factory Default
Enable/Disable	Adjusts the interference coping capability of the wireless signal. This option should be enabled for communication distance under 500 meters, and should be disabled for communication distances over 500 meters.	Enable

Transmission enhancement

Setting	Description	Factory Default
Enable/Disable	This setting can enhance communication by strengthening the IE-WL-AP-BR-CL-ABG's transmission power. It is quite useful for long-distance transmission or countering environmental interference. The user must carefully evaluate and measure the transmission power of the entire system to ensure it stays below the regulative limit. In addition, that RF type 802.11a mode cannot be used if this function is enabled.	Disable

NOTE When Transmission enhancement is enabled, the Tx Power is at "Full"

RF type = B/G/Mixed (Channel1~13)

- US model: 22 dB
- EU model: 20 dB

RF type = A (Channel 36 ~ 48)

- US model: 17 dB
- EU model: 17 dB

NOTE Make sure the same **Transmission distance** parameters are set in both **AP** and **Client** sides, and both **Bridges**. When this parameter is greater than 500, an optimal algorithm will be enabled to support long-distance transmission.

Note that **Transmission enhancement** only supports **802.11b/g** mode; **802.11a** mode is not supported.

Transmission enhancement is also recommended to enable communication at both ends when long-distance transmission is required. A high-gain antenna installed at a fixed antenna connector can also improve performance. (Select **Antenna** at MAIN or AUX.)

Antenna

Setting	Description	Factory Default
Auto	The IE-WL-AP-BR-CL-ABG uses two antennas (MAIN and AUX) and enables the diversity function for reducing multipath effect.	Auto
MAIN	Diversity function is disabled. Only MAIN antenna is in use.	
AUX	Diversity function is disabled. Only AUX antenna is in use.	

EAPOL Version

Setting	Description	Factory Default
1	EAPOL version 1 was standardized in the 2001 version of 802.1X, which is much more commonly implemented.	1
2	EAPOL version 2 was specified in 802.1X-2004.	

WMM

Setting	Description	Factory Default
Enable/Disable	WMM is a QoS standard for WLAN traffic. Voice and video data will be given priority bandwidth when enabled with WMM supported wireless clients.	Disable

Full 11a channel support

Setting	Description	Factory Default
Enable/Disable	"Full 11a channel support" allows users to select one channel from 802.11a, including channels in licensed and unlicensed bands.	Disable

READ THIS BEFORE CHANGING THE DFS SETTING

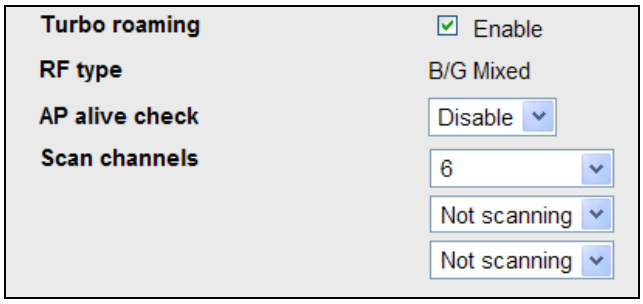
DFS (Dynamic Frequency Selection) is a mechanism to allow unlicensed wireless devices to share spectrum with existing radar systems by detecting radar systems and avoid causing interference with them. The current versions of Weidmüller IE-WL-AP-BR-CL-ABG products do not support DFS, so only U-NII Low channels (36, 40, 44, and 48) are supported by default. If you want to enable the "Full 11a channel support" option, keep in mind that your wireless devices may interfere with radar systems, which may violate local laws. If you are not sure about this, we recommend that you keep this option disabled. Updated firmware that supports DFS will be available soon.

Turbo Roaming (for Client mode only)

Setting	Description	Factory Default
Enable/ Disable	Turbo Roaming can enable rapid handover when the IE-WL-AP-BR-CL-ABG, as a client, roams among a group of APs.	Disable

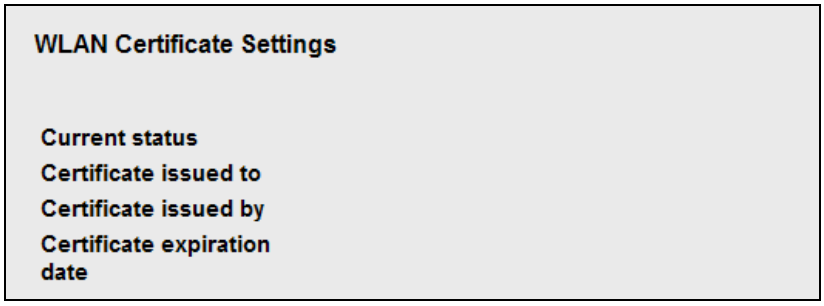
When Turbo Roaming is enabled, the RF type, AP alive check, and Scan channels will be shown as follows. RF type shows the current **RF type** that this client is using. **AP alive check** will check if the AP connection is still available. When this function is enabled, a check will be done every 10 ms. You can set up **Scan channels** for the APs among which this client is going to roam. There are three Scan channels available. Note that the **Scan**

channels may need to be modified when the **RF type** is changed. (For example, channel 36 is not available in **B**, **G**, or **B/G Mix** mode.)



WLAN Certification Settings (for EAP-TLS in Client mode only)

When EAP-TLS is used, a WLAN Certificate will be required at the client end to support WPA/WPA2-Enterprise. The IE-WL-AP-BR-CL-ABG can support the **PKCS #12**, also known as *Personal Information Exchange Syntax Standard*, certificate formats that define file formats commonly used to store private keys with accompanying public key certificates, protected with a password-based symmetric key.



Current Status displays information for the current WLAN certificate, which has been imported into the IE-WL-AP-BR-CL-ABG. Nothing will be shown if a certificate is not available.

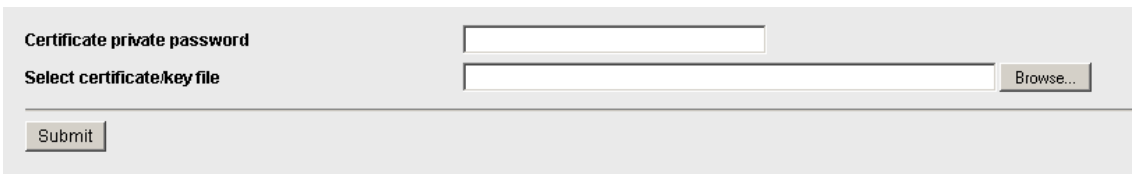
Certificate issued to: Shows the certificate user

Certificate issued by: Shows the certificate issuer

Certificate expiration date: Indicates when the certificate has expired

You can import a new WLAN certificate in ***Import WLAN Certificate*** by following these steps, in order:

1. Input the corresponding password (or key) in the **Certificate private password** field and then click **Submit** to set the password.
2. The password will be displayed in the Certificate private password field. Click on the **Browse** button in ***Select certificate/key file*** and select the certificate file.
3. Click **Upload Certificate File** to import the certificate file. If the import succeeds, you can see the information uploaded in ***Current Certificate***. If it fails, you may need to return to step 1 to set the password correctly and then import the certificate file again.



NOTE The WLAN certificate will remain after the IE-WL-AP-BR-CL-ABG reboots. Even though it is expired, it can still be seen on the ***Current Certificate***.

Advanced Settings

Several advanced functions are available to increase the functionality of your IE-WL-AP-BR-CL-ABG and wireless network system. A VLAN is a collection of clients and hosts grouped together as if they were connected to the broadcast domains in a layer 2 network. The DHCP server helps you deploy wireless clients efficiently. Packet filters provide security mechanisms, such as firewalls, in different network layers. Moreover, the IE-WL-AP-BR-CL-ABG can support STP/RSTP protocol to increase reliability across the entire network, and SNMP support can make network management easier.

Using Virtual LAN

Setting up Virtual LANs (VLANs) on your IE-WL-AP-BR-CL-ABG increases the efficiency of your network by dividing the LAN into logical segments, as opposed to physical segments. In general, VLANs are easier to manage.

The Virtual LAN (VLAN) Concept

What is a VLAN?

A virtual LAN, commonly known as a VLAN, is a group of hosts with a common set of requirements that communicate as if they were attached to the same broadcast domain, regardless of their physical location. A VLAN has the same attributes as a physical LAN, but it allows for end stations to be grouped together even if they are not located on the same network switch. Network reconfiguration can be done through software instead of physically relocating devices.

VLANs now extend as far as the reach of the access point signal. Clients can be segmented into wireless sub-networks via SSID and VLAN assignment. A Client can access the network by connecting to an AP configured to support its assigned SSID/VLAN.

Benefits of VLANs

VLANs are used to conveniently, efficiently, and easily manage your network in the following ways:

- Manage adds, moves, and changes from a single point of contact
- Define and monitor groups
- Reduce broadcast and multicast traffic to unnecessary destinations
- Improve network performance and reduce latency
- Increase security
- Secure network restricts members to resources on their own VLAN
- Clients roam without compromising security

VLAN Workgroups and Traffic Management

The AP assigns clients to a VLAN based on a Network Name (SSID). The AP can support up to 9 SSIDs per radio interface, with a unique VLAN configurable per SSID.

The AP matches packets transmitted or received to a network name with the associated VLAN. Traffic received by a VLAN is only sent on the wireless interface associated with that same VLAN. This eliminates unnecessary traffic on the wireless LAN, conserving bandwidth and maximizing throughput.

In addition to enhancing wireless traffic management, the VLAN-capable AP supports easy assignment of wireless users to workgroups. In a typical scenario, each user VLAN represents a department workgroup; for example, one VLAN could be used for a marketing department and the other for a human resource department.

In this scenario, the AP would assign every packet it accepted to a VLAN. Each packet would then be identified as marketing or human resource, depending on which wireless client received it. The AP would insert VLAN headers or “tags” with identifiers into the packets transmitted on the wired backbone to a network switch.

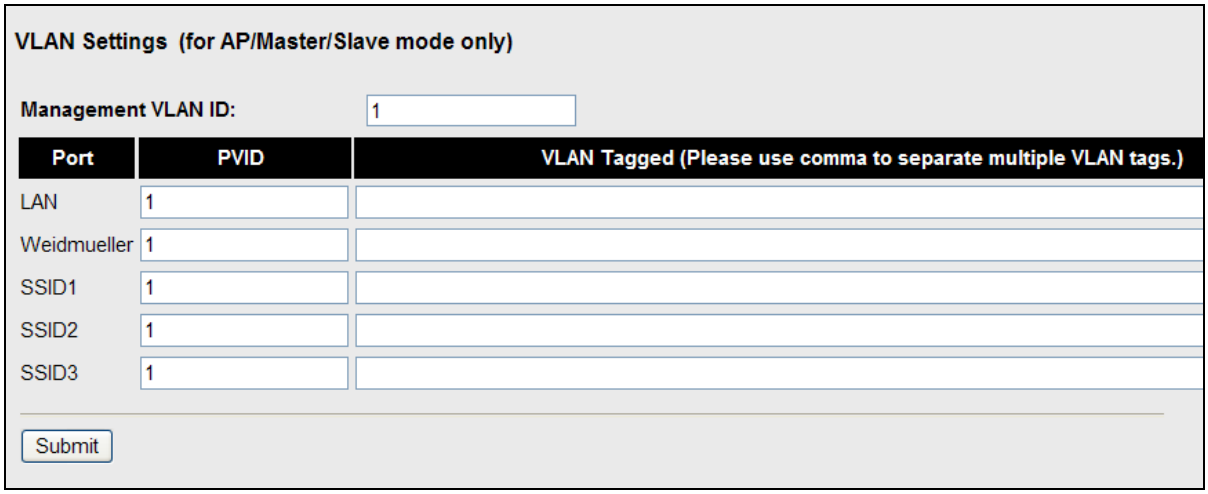
Finally, the switch would be configured to route packets from the marketing department to the appropriate corporate resources such as printers and servers. Packets from the human resource department could be restricted to a gateway that allowed access to only the Internet. A member of the human resource department

could send and receive e-mail and access the Internet, but would be prevented from accessing servers or hosts on the local corporate network.

Configuring Virtual LAN

VLAN Settings

To configure the IE-WL-AP-BR-CL-ABG's VLAN, use the VLAN Setting page to configure the ports.



Management VLAN ID

Setting	Description	Factory Default
VLAN ID ranges from 1 to 4094	Set the management VLAN of this IE-WL-AP-BR-CL-ABG.	1

Port

Type	Description	Trunk Port
LAN	This port is the LAN port on the IE-WL-AP-BR-CL-ABG.	Yes
WLAN	This is a wireless port for the specific SSID. This field will refer to the SSID that you have created. If more SSIDs have been created, new rows will be added.	
WDS	This is the WDS port on the IE-WL-AP-BR-CL-ABG	Yes

Port PVID

Setting	Description	Factory Default
VLAN ID ranging from 1 to 4094	Set the port's VLAN ID for devices that connect to the port. The port can be a LAN port or WLAN ports.	1

VLAN Tagged

Setting	Description	Factory Default
A comma-seperated list of VLAN IDs. Each of the VLAN IDs range from 1 to 4094.	Specify which VLANs can communicate with this specific VLAN.	(Empty)

NOTE The VLAN feature can allow wireless clients to manage the AP. If the VLAN Management ID matches a VLAN ID, then those wireless clients who are members of that VLAN will have AP management access.

CAUTION: Once a VLAN Management ID is configured and is equivalent to one of the VLAN IDs on the AP, all members of that User VLAN will have management access to the AP. Be careful to restrict VLAN membership

to those with legitimate access to the AP.

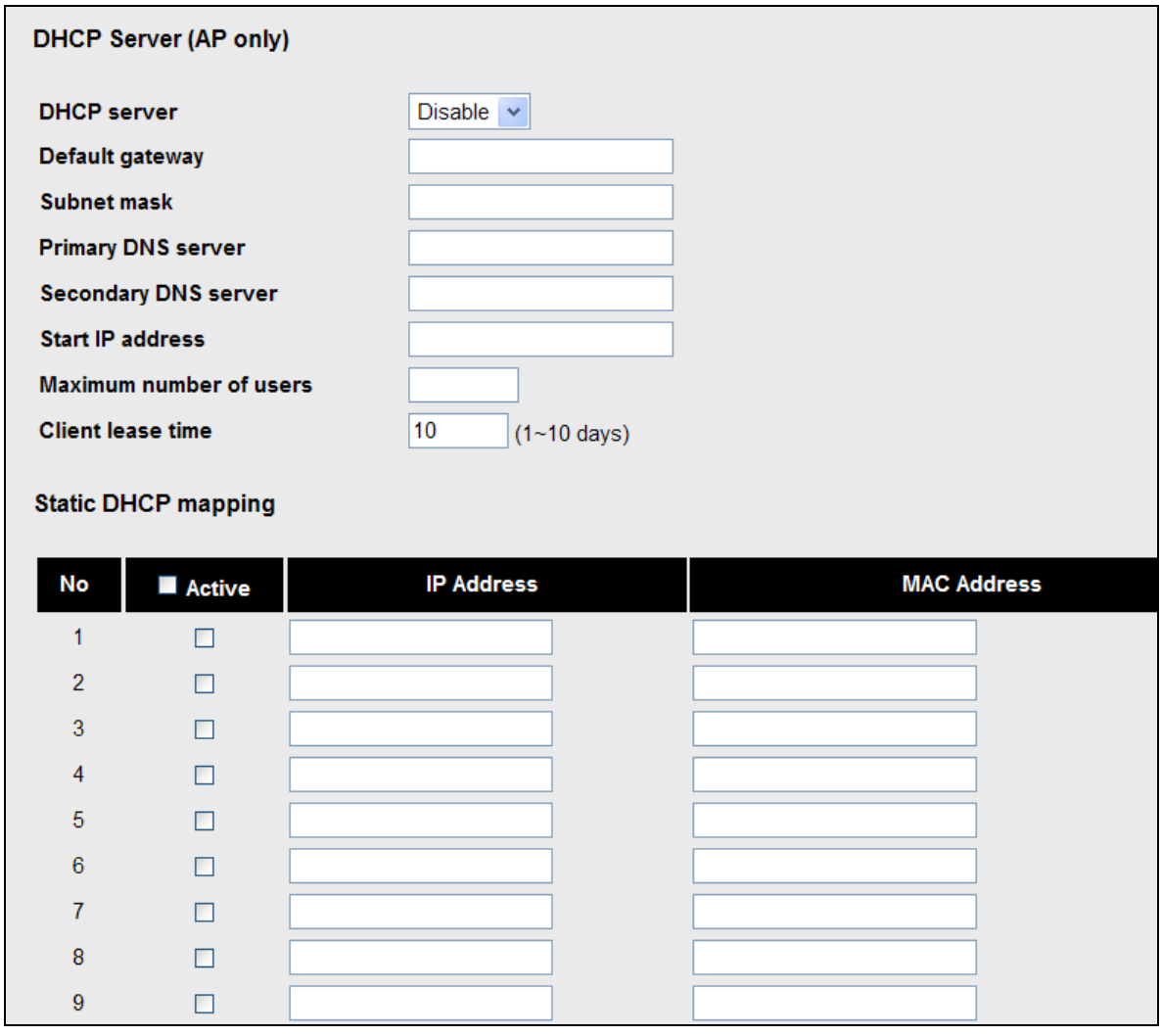
DHCP Server (for AP mode only)

DHCP (Dynamic Host Configuration Protocol) is a networking protocol that allows administrators to assign temporary IP addresses to network computers by "leasing" an IP address to a user for a limited amount of time, instead of assigning permanent IP addresses.

The IE-WL-AP-BR-CL-ABG can act as a simplified DHCP server and easily assign IP addresses to your wireless clients by responding to the DHCP requests from the client ends. The IP-related parameters you set on this page will also be sent to the client.

You can also assign a static IP address to a specific client by entering its MAC address. The IE-WL-AP-BR-CL-ABG provides a **Static DHCP mapping** list with up to 16 entities. Be reminded to check the **Active** check box for each entity to activate the setting.

You can check the IP assignment status under **Status → DHCP Client List**.



DHCP server

Setting	Description	Factory Default
Enable	Enables IE-WL-AP-BR-CL-ABG as a DHCP server	Disable
Disable	Disable DHCP server function	

Default gateway

Setting	Description	Factory Default

IP address of a default gateway	The IP address of the router that connects to an outside network	None

Subnet mask

Setting	Description	Factory Default
subnet mask	Identifies the type of sub-network (e.g., 255.255.0.0 for a Class B network, or 255.255.255.0 for a Class C network)	None

Primary / Secondary DNS server

Setting	Description	Factory Default
IP address of Primary/ Secondary DNS server	The IP address of the DNS Server used by your network. After entering the DNS Server's IP address, you can use URL as well. The Secondary DNS server will be used if the Primary DNS server fails to connect.	None

Start IP address

Setting	Description	Factory Default
IP address	Indicates the IP address which IE-WL-AP-BR-CL-ABG can start assigning	None

Maximum number of users

Setting	Description	Factory Default
1 – 999	Specifies how many IP address can be assigned continuously	None

Client lease time

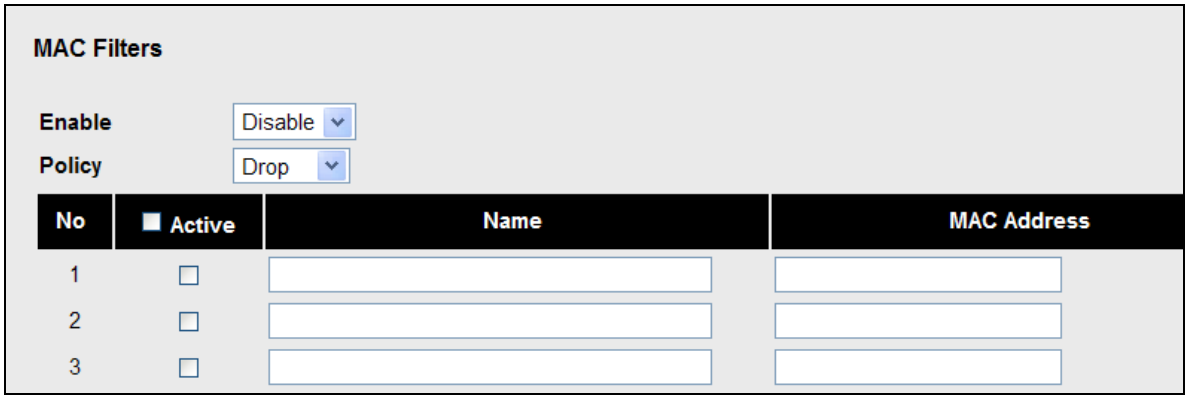
Setting	Description	Factory Default
1 – 10 days	The lease time for which an IP address is assigned. The IP address may go expired after the lease time is reached.	10 (days)

Packet Filters

The IE-WL-AP-BR-CL-ABG includes various filters for **IP-based** packets going through LAN and WLAN interfaces. You can set these filters as a firewall to help enhance network security.

MAC Filter

The IE-WL-AP-BR-CL-ABG's MAC filter is a policy-based filter that can allow or filter out IP-based packets with specified MAC addresses. The IE-WL-AP-BR-CL-ABG provides 8 entities for setting MAC addresses in your filtering policy. Remember to check the **Active** check box for each entity to activate the setting.



Enable

Setting	Description	Factory Default
Enable	Enables MAC filter	Disable
Disable	Disables MAC filter	

Policy

Setting	Description	Factory Default
Accept	Only the packets fitting the entities on list can be allowed.	Drop
Drop	Any packet fitting the entities on list will be denied.	

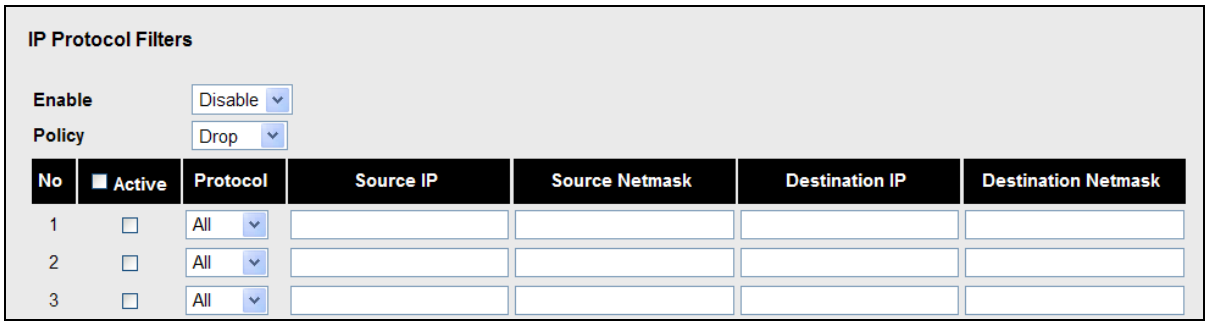
ATTENTION

Be careful when you enable the filter function:
Drop + "no entity on list is activated" = all packets are **allowed**
Accept + "no entity on list is activated" = all packets are **denied**

IP Protocol Filter

The IE-WL-AP-BR-CL-ABG's IP protocol filter is a policy-based filter that can allow or filter out IP-based packets with specified IP protocol and source/destination IP addresses.

The IE-WL-AP-BR-CL-ABG provides 8 entities for setting IP protocol and source/destination IP addresses in your filtering policy. Four IP protocols are available: **All**, **ICMP**, **TCP**, and **UDP**. You must specify either the Source IP or the Destination IP. By combining IP addresses and netmasks, you can specify a single IP address or a range of IP addresses to accept or drop. For example, "IP address 192.168.1.1 and netmask 255.255.255.255" refers to the sole IP address 192.168.1.1. "IP address 192.168.1.1 and netmask 255.255.255.0" refers to the range of IP addresses from 192.168.1.1 to 192.168.255. Remember to check the **Active** check box for each entity to activate the setting.



Enable

Setting	Description	Factory Default
Enable	Enables IP protocol filter	Disable
Disable	Disables IP protocol filter	

Policy

Setting	Description	Factory Default
Accept	Only the packets fitting the entities on the list can be allowed	Drop
Drop	Any packet fitting the entities on the list will be denied	

ATTENTION

Be careful when you enable the filter function:
Drop + "no entity on list is activated" = all packets are **allowed.**
Accept + "no entity on list is activated" = all packets are **denied.**

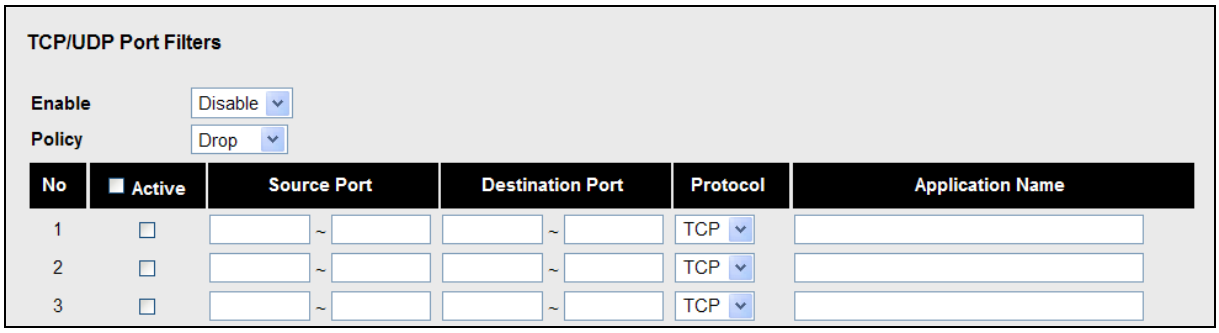
TCP/UDP Port Filter

The IE-WL-AP-BR-CL-ABG's TCP/UDP port filter is a policy-based filter that can allow or filter out TCP/UDP-based packets with a specified source or destination port.

The IE-WL-AP-BR-CL-ABG provides 8 entities for setting the range of source/destination ports of a specific protocol. In addition to selecting TCP or UDP protocol, you can set either the source port, destination port, or

both. The end port can be left empty if only a single port is specified. Of course, the end port cannot be larger then the start port.

The **Application name** is a text string that describes the corresponding entity with up to 31 characters. Remember to check the **Active** check box for each entity to activate the setting.



Enable

Setting	Description	Factory Default
Enable	Enables TCP/UDP port filter	Disable
Disable	Disables TCP/UDP port filter	

Policy

Setting	Description	Factory Default
Accept	Only the packets fitting the entities on list can be allowed.	Drop
Drop	Any packet fitting the entities on list will be denied.	

ATTENTION

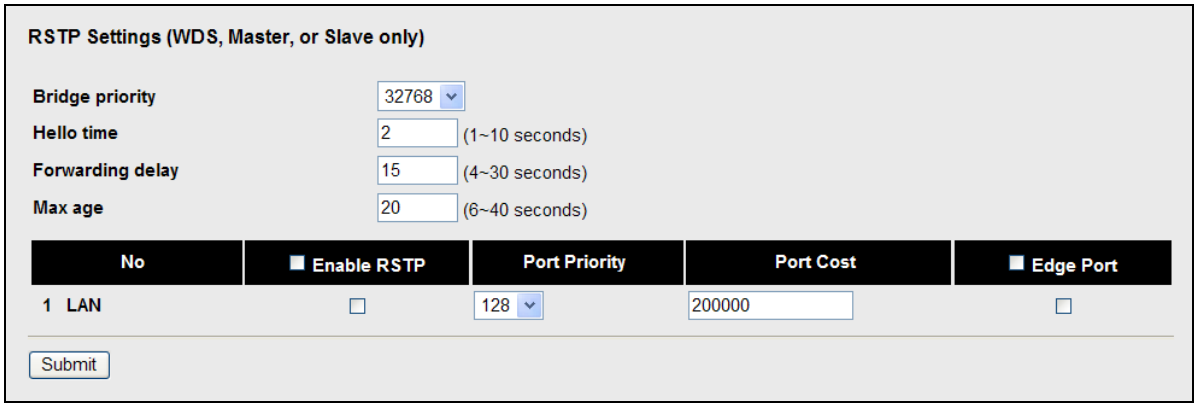
Be careful when you enable the filter function:
Drop + "no entity on list is activated" = all packets are **allowed**
Accept + "no entity on list is activated" = all packets are **denied**

RSTP Settings (for AP mode only)

IE-WL-AP-BR-CL-ABG supports IEEE802.1D Spanning Tree Protocol and IEEE802.1w Rapid STP standards. In addition to eliminating unexpected path looping, STP/RSTP can provide a backup path recovery if a wired/ wireless path fails accidentally. The reliability and availability can increase because this fail-over function.

IE-WL-AP-BR-CL-ABG's STP/RSTP feature is disabled by default. To be completely effective, you must enable RSTP/STP on every IE-WL-AP-BR-CL-ABG connected to your network. If IE-WL-AP-BR-CL-ABG plays a **Client** role, which is connected to a device (PLC, RTU, etc.) as opposed to network switch equipment, it is not necessary to enable STP/RSTP. The reason is that it will cause unnecessary negotiation. IE-WL-AP-BR-CL-ABGs support STP/RSTP in **AP** mode (including WDS) only.

The following figures indicate which Spanning Tree Protocol parameters can be configured. A more detailed explanation of each parameter is given below the figure.



RSTP status

This field will appear only when selected to operate STP/RSTP. It indicates whether this IE-WL-AP-BR-CL-ABG is the Root of the Spanning Tree (the root is determined automatically) or not.

Bridge priority

Setting	Description	Factory Default
Numerical value selected by user	You can increase the bridge priority by selecting a lower number. A higher bridge priority brings a greater chance of being established as the root of the Spanning Tree topology.	32768

Hello time

Setting	Description	Factory Default
Numerical value input by user (1 – 10 seconds)	The root of the Spanning Tree topology periodically sends out a "hello" message to other devices on the network to check if the topology is healthy. Hello time indicates how often the root sends hello messages.	2 (seconds)

Forwarding delay

Setting	Description	Factory Default
Numerical value input by user (4 – 30 seconds)	The amount of time this device waits before checking to see if it should change to a different topology.	15 (seconds)

Max. age

Setting	Description	Factory Default
Numerical value input by user (6 – 40 seconds)	As a non-root role, if the device has not received a hello message from the root longer than Max. age, it will reconfigure itself as a root. Once two or more devices on the network are recognized as a root, the devices will renegotiate to set up a new Spanning Tree topology.	20 (seconds)

The IE-WL-AP-BR-CL-ABG comes with 10 "ports" for RSTP settings. Numbers 3-10 (WDS1-WDS8) are available only when WDS is enabled in AP mode.

Enable RSTP

Setting	Description	Factory Default
Enable/ disable	Enables or disables the port as a node on the Spanning Tree topology.	Disable (unchecked)

Port priority

Setting	Description	Factory Default
Numerical value selected by user	Increase this port's priority as a node on the Spanning Tree topology by inputting a lower number.	128

Port cost

Setting	Description	Factory Default
Enable/ Disable	Input a higher cost to indicate that this port is less suitable as a node for the Spanning Tree topology	2000000

Edge port

Setting	Description	Factory Default
Checked/ unchecked	Sets a port, which no BPDU expectedly goes through, as an edge port	unchecked, except AP port

NOTE We recommend you set an edge port for the port, which is connected to a non-STP/RSTP sub-network or an end device (PLC, RTU, etc.) as opposed to network equipment. This can prevent unnecessary waiting and negotiation of STP/RSTP protocol, and accelerate system initialization. When an edge port receives BPDUs, it can still function as an STP/RSTP port and start negotiation.
Setting an edge port is different from disabling STP/RSTP on a port. If you disable STP/RSTP, a port will not deal with STP/RSTP BPDUs at all.

Port Status

Port Status indicates the current Spanning Tree status of this port. Use **Forwarding** for normal transmission, or **Blocking** to block transmission.

SNMP Agent

The IE-WL-AP-BR-CL-ABG supports SNMP V1/V2c/V3. SNMP V1 and SNMP V2c use a community string match for authentication, which means that SNMP servers access all objects with read-only or read/write permissions using the community string *public*/*private* (default value). SNMP V3, which requires you to select an authentication level of MD5 or SHA, is the most secure protocol. You can also enable data encryption to enhance data security.

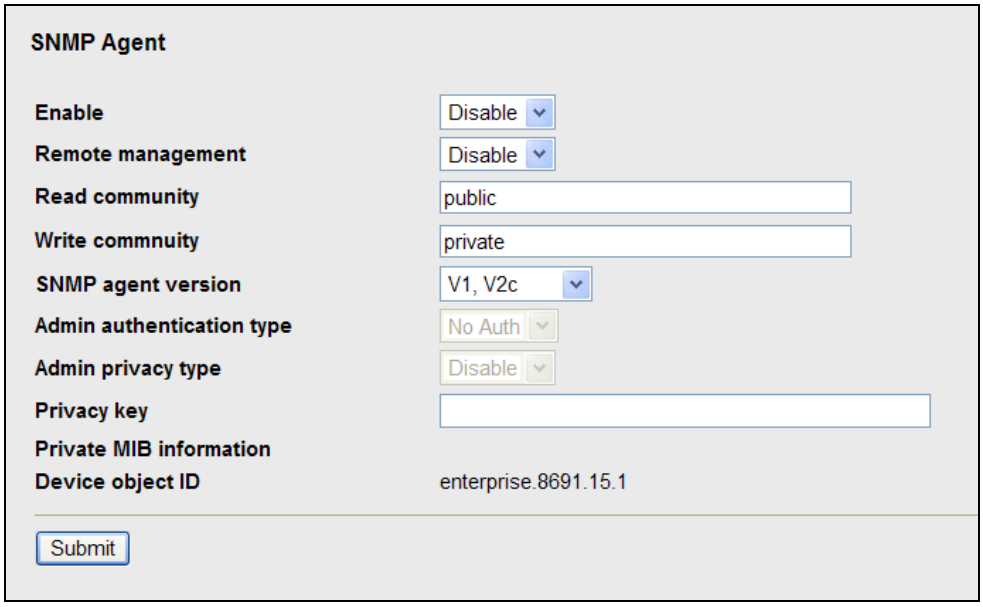
The IE-WL-AP-BR-CL-ABG's MIB can be found on www.weidmueller.com/Downloads/Software/Industrial-Ethernet and supports reading the attributes via SNMP. (Only ***get*** method is supported.)

SNMP security modes and security levels supported by the IE-WL-AP-BR-CL-ABG are shown in the following table. Select the security mode and level that will be used to communicate between the SNMP agent and manager.

Protocol Version	Setting on UI web page	Authentication Type	Data Encryption	Method
SNMP V1, V2c	V1, V2c Read Community	Community string	No	Use a community string match for authentication
	V1, V2c Write/Read Community	Community string	No	Use a community string match for authentication
SNMP V3	No-Auth	No	No	Use account with admin or user to access objects
	MD5 or SHA	Authentication based on MD5 or SHA	No	Provides authentication based on HMAC-MD5, or HMAC-SHA algorithms. 8-character passwords are the minimum requirement for authentication.
	MD5 or SHA	Authentication based on MD5 or SHA	Data encryption key	Provides authentication based on HMAC-MD5 or HMAC-SHA algorithms, and data encryption key. 8-character passwords and a data encryption key are the minimum

				requirements for authentication and encryption.

The following parameters can be configured on the **SNMP Agent** page. A more detailed explanation of each parameter is given below the following figure.



Enable

Setting	Description	Factory Default
Enable	Enables SNMP Agent	Disable
Disable	Disables SNMP Agent	

Remote Management

Setting	Description	Factory Default
Enable	Allow remote management via SNMP agent	Disable
Disable	Disallow remote management via SNMP agent	

Read community (for V1, V2c)

Setting	Description	Factory Default
V1, V2c Read Community	Use a community string match with a maximum of 31 characters for authentication. This means that the SNMP agent can access all objects with read-only permissions using this community string.	public

Write community (for V1, V2c)

Setting	Description	Factory Default
V1, V2c Read /Write Community	Use a community string match with a maximum of 31 characters for authentication. This means that the SNMP agent can accesses all objects with read/write permissions using this community string.	private

SNMP agent version

Setting	Description	Factory Default
V1, V2c, V3, or V1, V2c, or V3 only	Select the SNMP protocol version used to manage the switch.	V1, V2c

Admin auth type (for V1, V2c, V3, and V3 only)

Setting	Description	Factory Default
No Auth	Use admin account to access objects. No authentication	No Auth

MD5	Provide authentication based on the HMAC-MD5 algorithms. 8-character passwords are the minimum requirement for authentication.	
SHA	Provides authentication based on HMAC-SHA algorithms. 8-character passwords are the minimum requirement for authentication.	

Admin private key (for V1, V2c, V3, and V3 only)

Setting	Description	Factory Default
Disable	No data encryption	Disable
DES	DES-based data encryption	
AES	AES-based data encryption	

Private key

A data encryption key is the minimum requirement for data encryption (maximum of 63 characters)

Private MIB Information Device Object ID

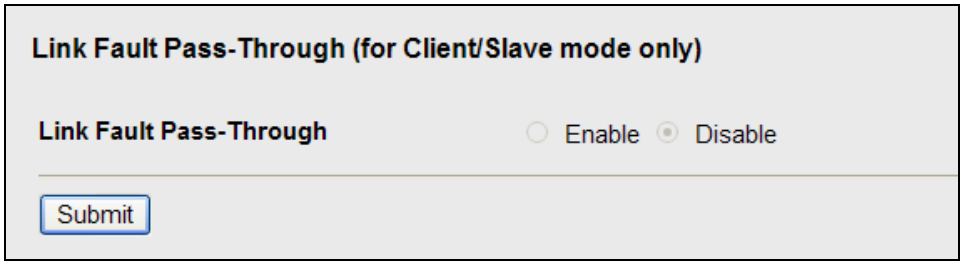
Also know as ***OID***. This is the IE-WL-AP-BR-CL-ABG's enterprise value. It is fixed.

Link Fault Pass-Through (for Client/Slave mode only)

This function means if Ethernet port is link down, wireless connection will be forced to disconnect. Once Ethernet link is recovered, IE-WL-AP-BR-CL-ABG will try to connect to AP.

If wireless is disconnected, IE-WL-AP-BR-CL-ABG restarts auto-negotiation on Ethernet port but always stays in the link failure state. Once the wireless connection is recovered, IE-WL-AP-BR-CL-ABG will try to recover the Ethernet link.

System log will indicate the link fault pass through events in addition to the original link up/down events.



Link Fault Pass-Through

Setting	Description	Factory Default
Enable	Enables Link Fault Pass-Through	Disable
Disable	Disable Link Fault Pass-Through	

Auto Warning Settings

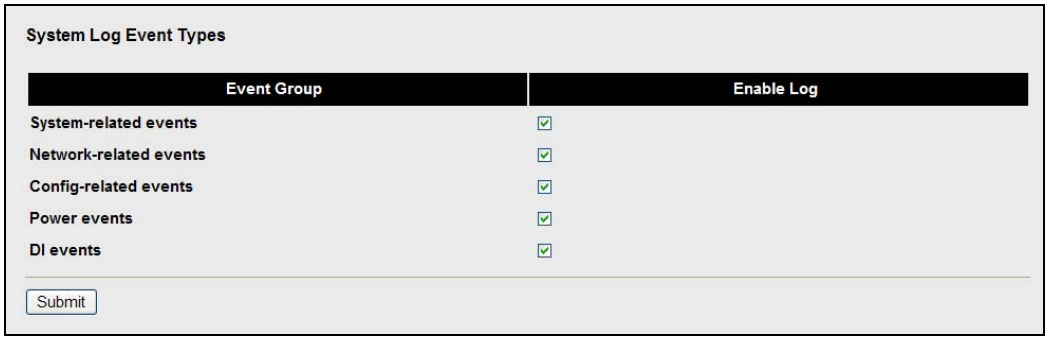
Since industrial-grade devices are often located at the endpoints of a system, these devices will not always know what is happening elsewhere on the network. This means that these devices, including wireless APs or clients, must provide system maintainers with real-time alarm messages. Even when system administrators are out of the control room for an extended period, they can still be informed of the status of devices almost instantaneously when exceptions occur.

In addition to logging these events, the IE-WL-AP-BR-CL-ABG supports different approaches to warn engineers automatically, such as SNMP trap, e-mail, and relay output. It also supports two digital inputs to integrate sensors into your system to automate alarms by email and relay output.

System Log

System Log Event Types

Detail information for grouped events is shown in the following table. You can check the box for Enable log to enable the grouped events. All default values are enabled (checked). The log for system events can be seen in Status → System Log.



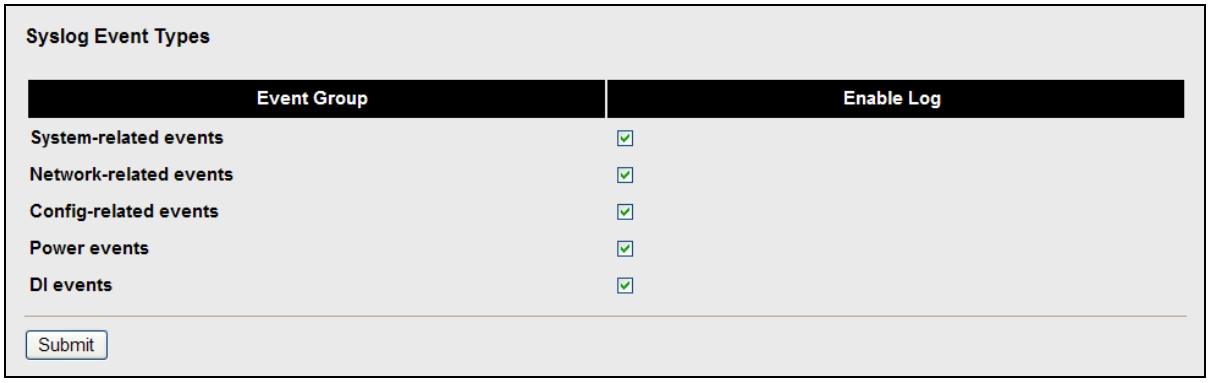
System-related events	**Event is triggered when…**
System restart (warm start)	The IE-WL-AP-BR-CL-ABG is rebooted, such as when its settings are changed (IP address, subnet mask, etc.).
Network-related events	**Event is triggered when…**
LAN link on	The LAN port is connected to a device or network.
LAN link off	The port is disconnected (e.g., the cable is pulled out, or the opposing device shuts down).
Client joined/ left (for AP/Master mode)	A wireless client is associated or disassociated.
WLAN connected to AP (for Client/Slave mode)	The IE-WL-AP-BR-CL-ABG is associated with an AP.
WLAN disconnected (for Client/Slave mode)	The IE-WL-AP-BR-CL-ABG is disassociated from an AP.
Config-related events	**Event is triggered when…**
Configuration Changed	A configuration item has been changed.
Configuration file import via Web Console	The configuration file is imported to the IE-WL-AP-BR-CL-ABG.
Console authentication failure	An incorrect password is entered.
Firmware upgraded	The IE-WL-AP-BR-CL-ABG's firmware is updated.
Power events	**Event is triggered when…**
Power 1/2 transition (On -> Off)	The IE-WL-AP-BR-CL-ABG is powered down in PWR1/2.
PoE transition (On -> Off)	The IE-WL-AP-BR-CL-ABG is powered down in PoE.
Power 1/2 transition (Off -> On)	The IE-WL-AP-BR-CL-ABG is powered via PWR1/2.
PoE transition (Off -> On)	The IE-WL-AP-BR-CL-ABG is powered via PoE.
DI events	**Event is triggered when…**
DI1/2 transition (On -> Off)	Digital Input 1/2 is triggered by on to off transition
DI1/2 transition (Off -> On)	Digital Input 1/2 is triggered by off to on transition

Syslog

This function provides the event logs for the Syslog server. The function supports up to three configurable Syslog servers and Syslog server UDP port numbers. When an event occurs, the event will be sent as a Syslog UDP packet to the specified Syslog servers.

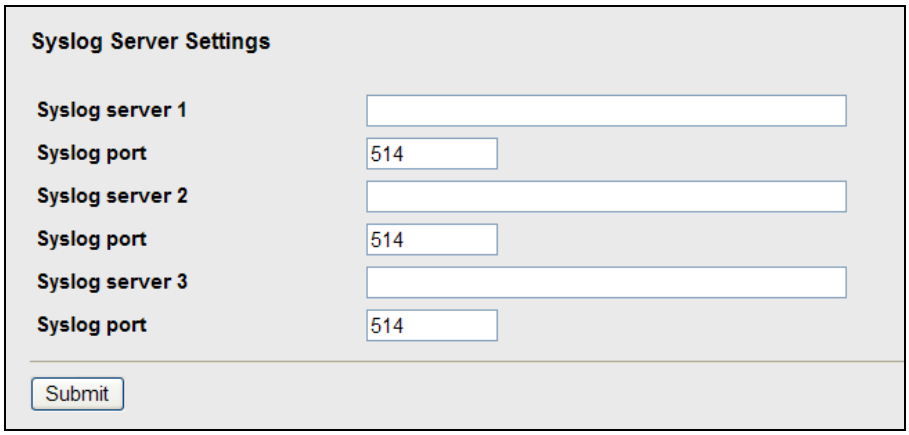
Syslog Event Types

Detail information for the grouped events is shown in the following table. You can check the box for **Enable log** to enable the grouped events. All default values are enabled (checked). Details for each event group can be found on the "System log Event Types" table on page 3-31.



Syslog Server Settings

You can configure the parameters for your Syslog servers in this page.



Syslog server 1 / 2 / 3

Setting	Description	Factory Default
IP address	Enter the IP address of the 1st/ 2nd/ 3rd Syslog Server	None

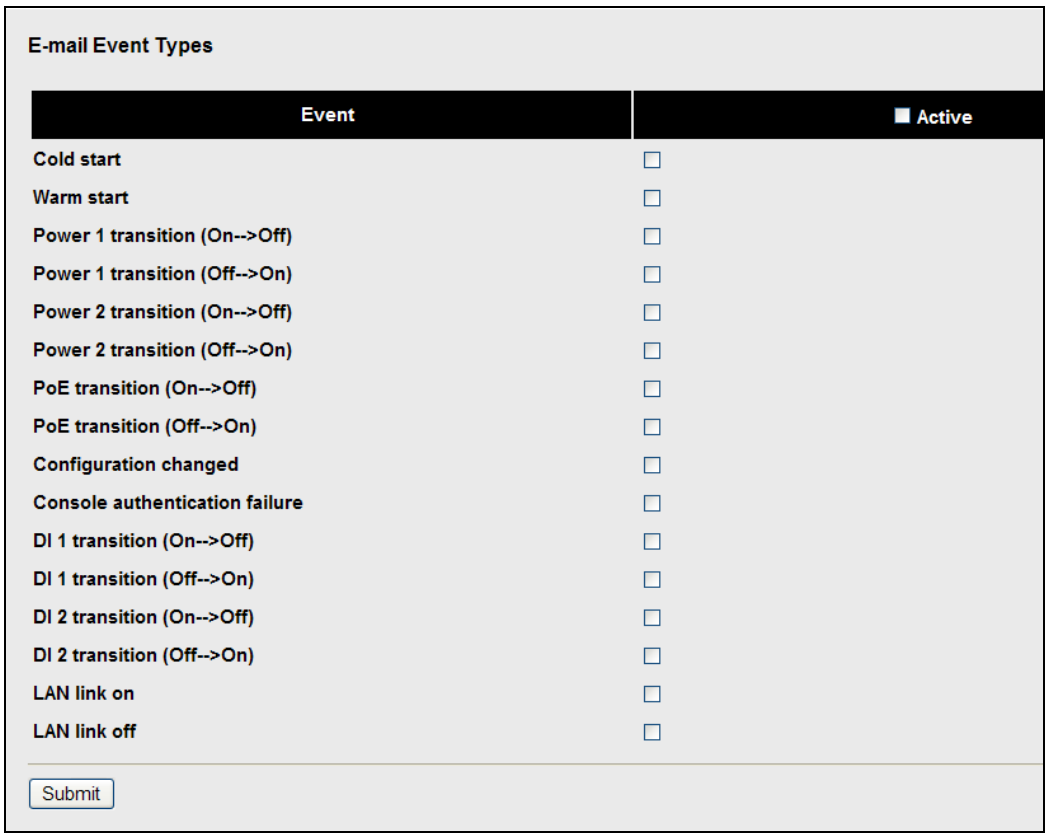
Syslog port

Setting	Description	Factory Default
Port destination (1 to 65535)	Enter the UDP port of the corresponding Syslog server	514

E-mail

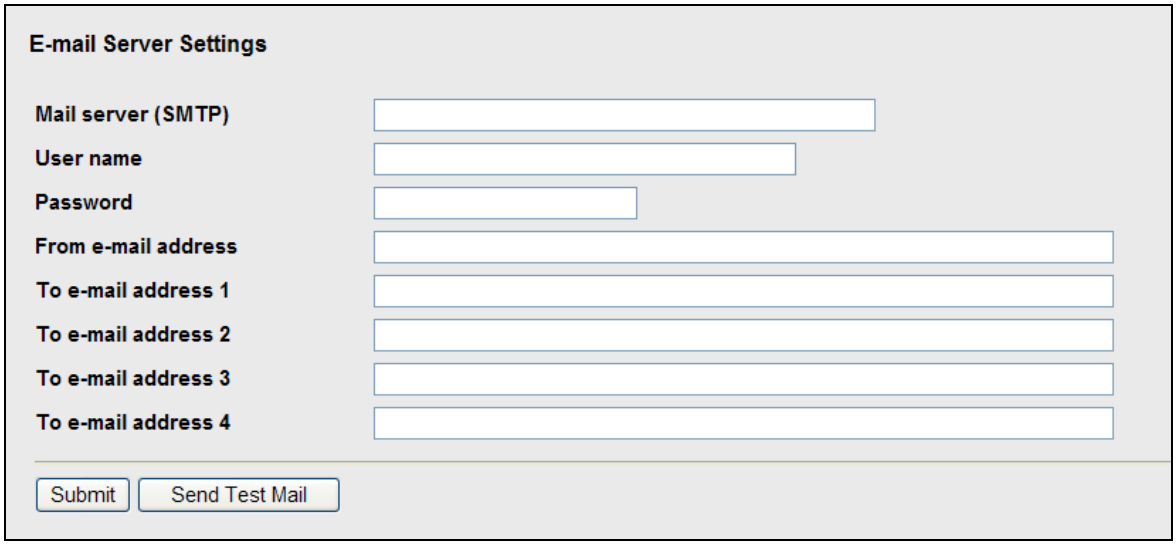
E-mail Event Types

Check the box for **Active** to enable the event items. All default values are deactivated (unchecked). Details for each event item can be found on the "System log Event Types" table on page 3-31.



E-mail Server Settings

You can set up to 4 e-mail addresses to receive alarm emails from the IE-WL-AP-BR-CL-ABG. The following parameters can be configured on the **E-mail Server Settings** page. In addition, a **Send Test Mail** button can be used to test whether the Mail server and e-mail addresses work well. More detailed explanations about these parameters are given after the following figure.



Mail server (SMTP)

Setting	Description	Factory Default
IP address	The IP Address of your email server.	None

User name & Password

Setting	Description	Factory Default
	User name and password used in the SMTP server	None

From e-mail address

Setting	Description	Factory Default
Max. 63 characters	Enter the administrator's e-mail address which will be shown in the "From" field of a warning e-mail.	None

To E-mail address 1 / 2 / 3 / 4

Setting	Description	Factory Default
Max. 63 characters	Enter the receivers' e-mail addresses.	None

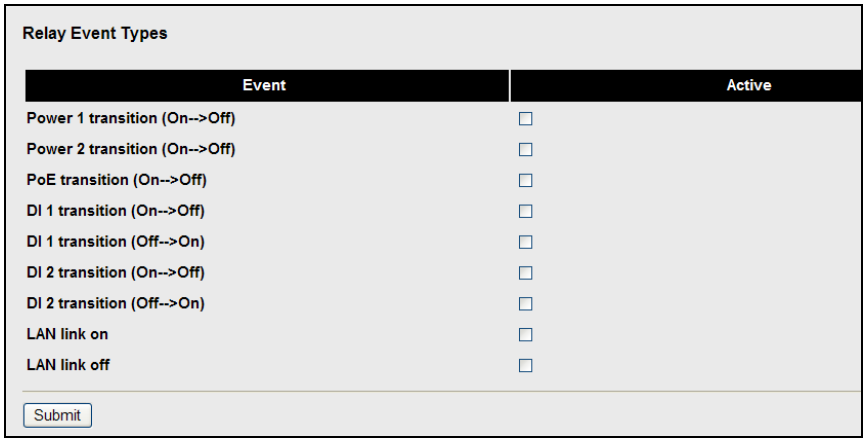
Relay

The IE-WL-AP-BR-CL-ABG has one relay output, which consists of 2 terminal block contacts on the IE-WL-AP-BR-CL-ABG's top panel. These relay contacts are used to indicate user-configured events and system failure.

The two wires attached to the relay contacts form an open circuit when a user-configured event is triggered. If a user-configured event does not occur, the relay circuit will remain closed. For safety reasons, the relay circuit is kept open when the IE-WL-AP-BR-CL-ABG is not powered.

Relay Event Types

You can check the box for **Active** to enable the event items. All default values are deactivated (unchecked). Details for each event item can be found in the "System log Event Types" table on page 3-31.

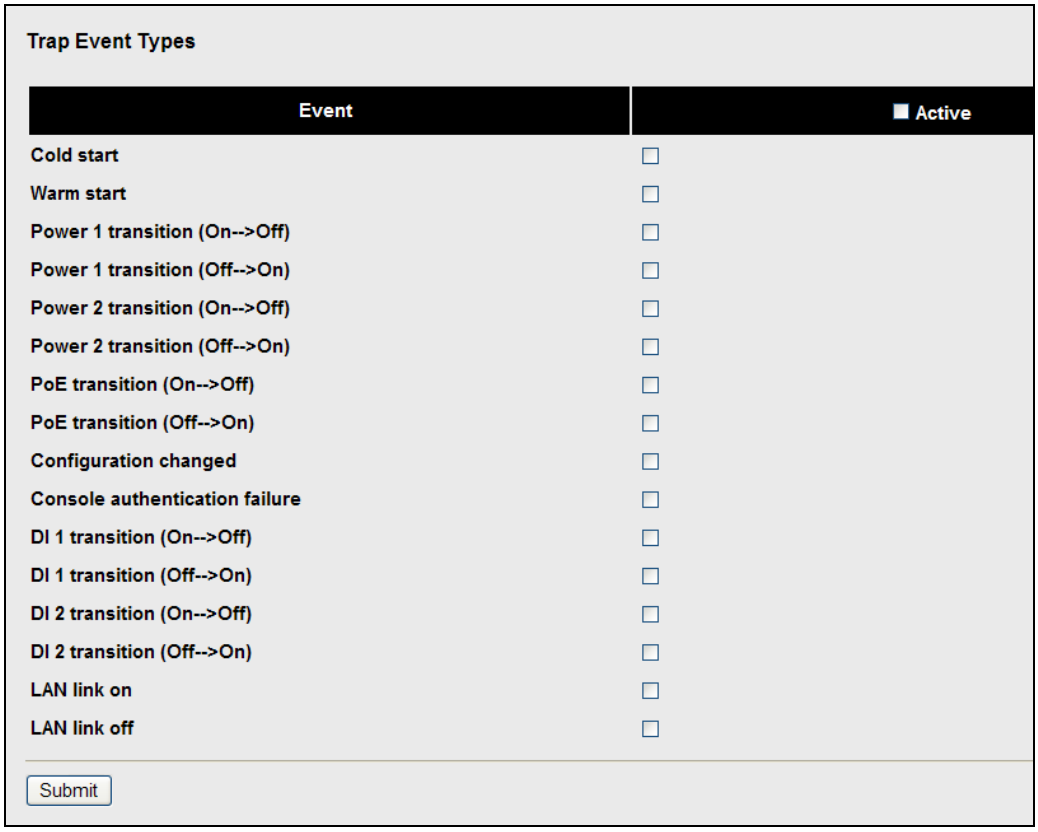


Trap

Traps can be used to signal abnormal conditions (notifications) to a management station. This trap-driven notification can make your network more efficient.

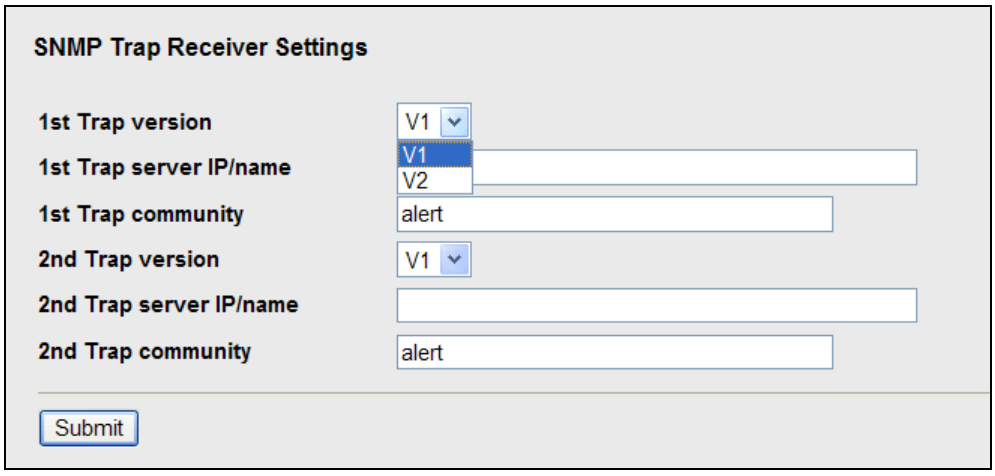
Because a management station usually takes care of a large number of devices that have a large number of objects, it will be overloading for the management station to poll or send requests to query every object on every device. It would be better if the managed device agent could notify the management station by sending a message known as a trap for the event.

Trap Event Types



SNMP Trap Receiver Settings

SNMP traps are defined in SMIv1 MIBs (SNMPv1) and SMIv2 MIBs (SNMPv2c). The two styles are basically equivalent, and it is possible to convert between the two. You can set the parameters for SNMP trap receivers through the web page.



1st / 2nd Trap version

Setting	Description	Factory Default
V1	SNMP trap defined in SNMPv1	V1
V2	SNMP trap defined in SNMPv2	

1st / 2nd Trap server IP/name

Setting	Description	Factory Default
IP address or host name	Enter the IP address or name of the trap server used by your network.	None

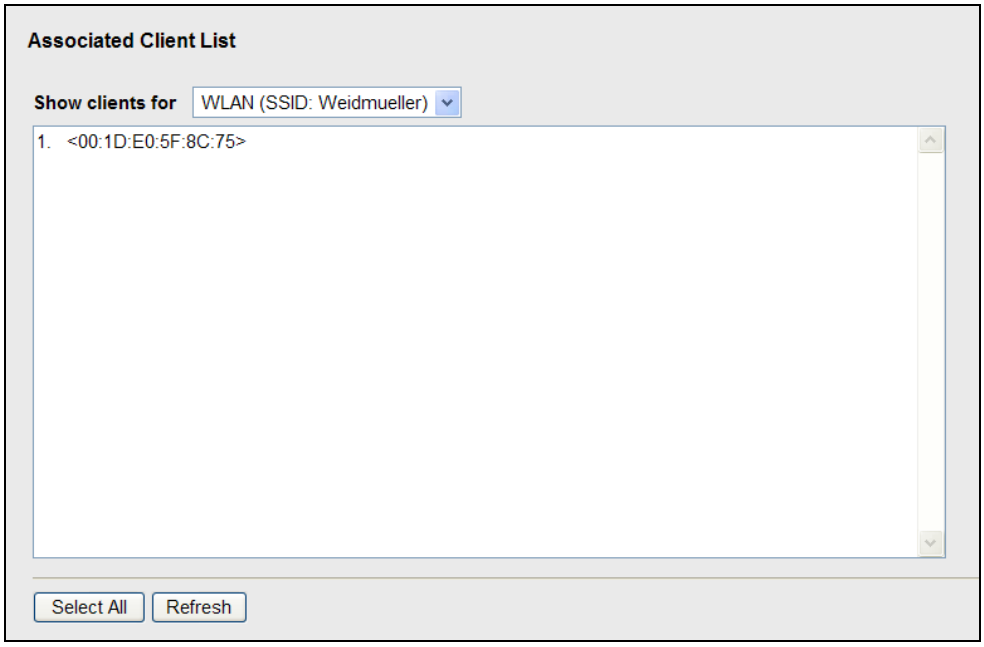
1st / 2nd Trap community

Setting	Description	Factory Default
Max. of 31 characters	Use a community string match with a maximum of 31 characters for authentication.	alert

Status

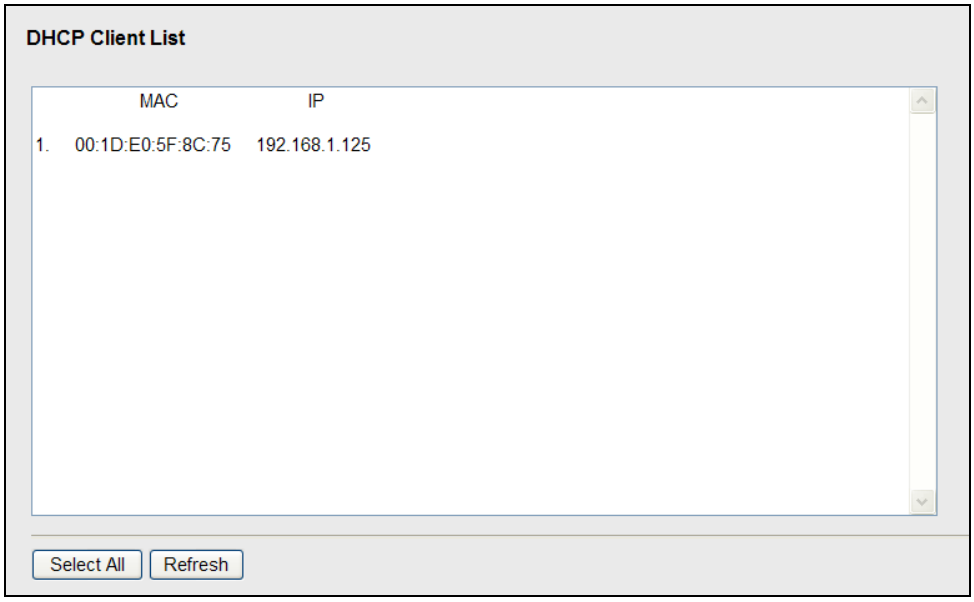
Associated Client List (for AP mode only)

Associated Client List shows all the clients that are currently associated to a particular IE-WL-AP-BR-CL-ABG. You can click **Select all** to select all the content in the list for further editing. You can click **Refresh** to refresh the list.

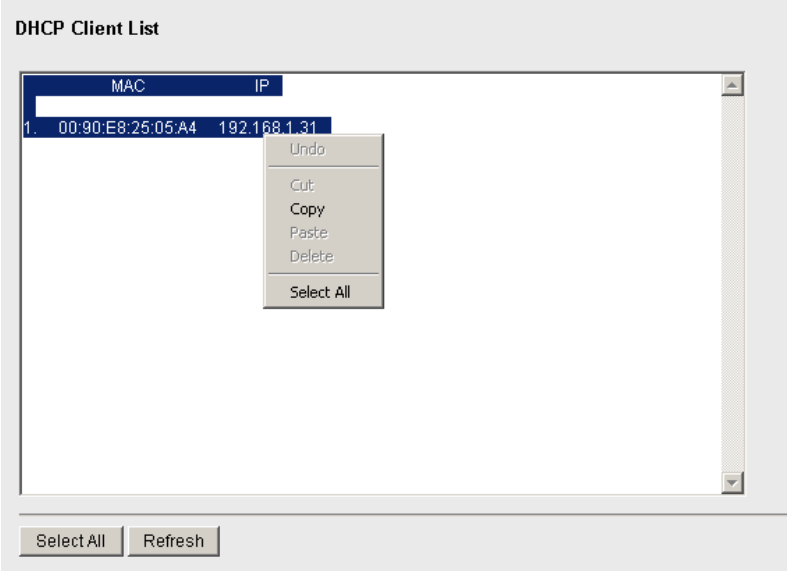


DHCP Client List (for AP mode only)

The DHCP Client List shows all the clients that require and have successfully received IP assignments. You can click the **Refresh** button to refresh the list.

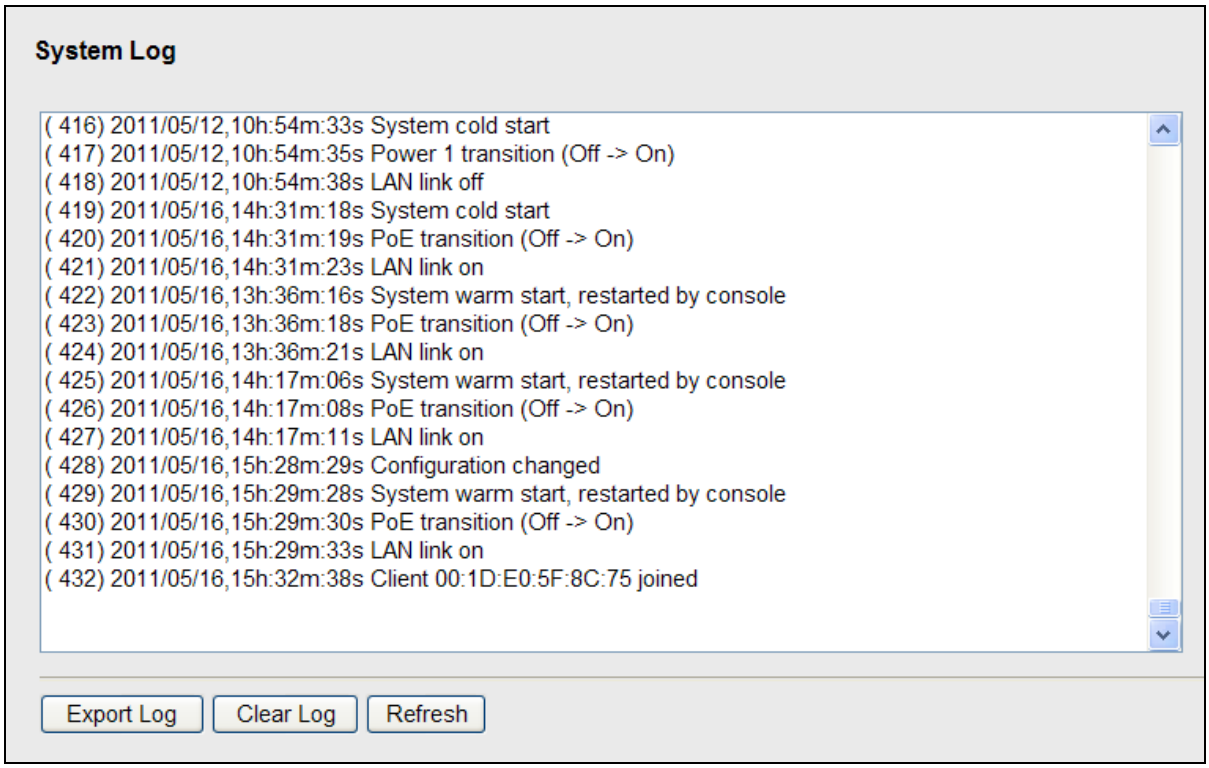


You can press **Select all** button to select all content in the list for further editing.



System Log

Triggered events are recorded in System Log. You can export the log contents to an available viewer by clicking **Export Log**. You can use the **Clear Log** button to clear the log contents and the **Refresh** button to refresh the log.


System Log
(416) 2011/05/12,10h:54m:33s System cold start
(417) 2011/05/12,10h:54m:35s Power 1 transition (Off -> On)
(418) 2011/05/12,10h:54m:38s LAN link off
(419) 2011/05/16,14h:31m:18s System cold start
(420) 2011/05/16,14h:31m:19s PoE transition (Off -> On)
(421) 2011/05/16,14h:31m:23s LAN link on
(422) 2011/05/16,13h:36m:16s System warm start, restarted by console
(423) 2011/05/16,13h:36m:18s PoE transition (Off -> On)
(424) 2011/05/16,13h:36m:21s LAN link on
(425) 2011/05/16,14h:17m:06s System warm start, restarted by console
(426) 2011/05/16,14h:17m:08s PoE transition (Off -> On)
(427) 2011/05/16,14h:17m:11s LAN link on
(428) 2011/05/16,15h:28m:29s Configuration changed
(429) 2011/05/16,15h:29m:28s System warm start, restarted by console
(430) 2011/05/16,15h:29m:30s PoE transition (Off -> On)
(431) 2011/05/16,15h:29m:33s LAN link on
(432) 2011/05/16,15h:32m:38s Client 00:1D:E0:5F:8C:75 joined
Export Log
Clear Log
Refresh

Relay Status

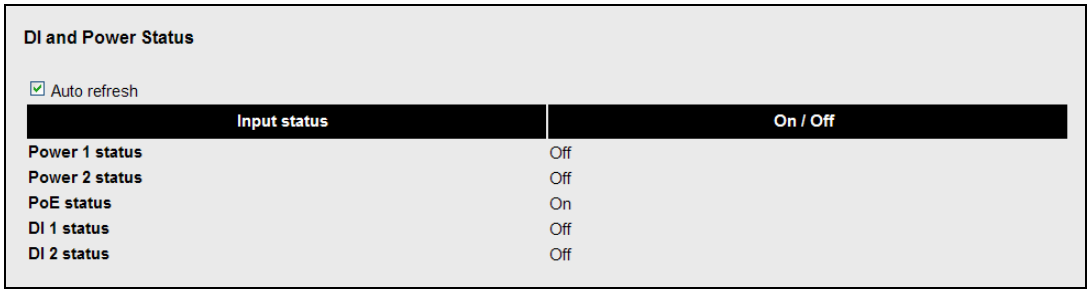
The status of user-configurable events can be found under **Relay Status**. The status will refresh every 5 seconds if the **Auto refresh** box is checked.

If an event is triggered, it will be noted on this list. System administrators can click **Acknowledge Event** when he has acknowledged the event and addressed it.

Relay Status
Auto refresh
Relay Status
Power 1 transition (On-->Off) --- Acknowledge Event
Power 2 transition (On-->Off) --- Acknowledge Event
PoE transition (On-->Off) --- Acknowledge Event
DI 1 transition (On-->Off) --- Acknowledge Event
DI 1 transition (Off-->On) --- Acknowledge Event
DI 2 transition (On-->Off) --- Acknowledge Event
DI 2 transition (Off-->On) --- Acknowledge Event
LAN link on --- Acknowledge Event
LAN link off --- Acknowledge Event

DI and Power Status

The status of power inputs and digital inputs is shown on this web page. The status will refresh every 5 seconds if the **Auto refresh** box is checked.

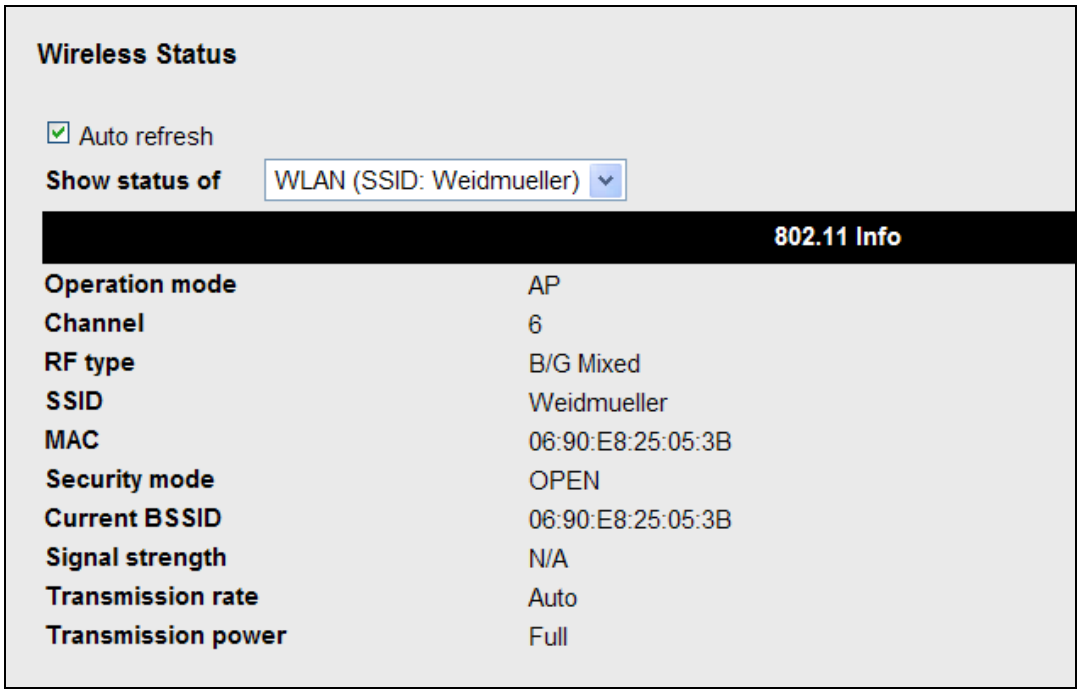


Wireless Status

The status for **802.11 info** parameters, such as Operation mode and Channel, are shown on the **Wireless Status** page. The status will refresh every 5 seconds if the **Auto refresh** box is checked.

Certain values for **802.11 info** may not show up due to different operation modes. As a result, **Current BSSID** and **Signal strength** are not available in AP mode.

It is helpful to use the continuously updated information on this page, such as **Signal strength**, to monitor the signal strength of the IE-WL-AP-BR-CL-ABG in Client mode.

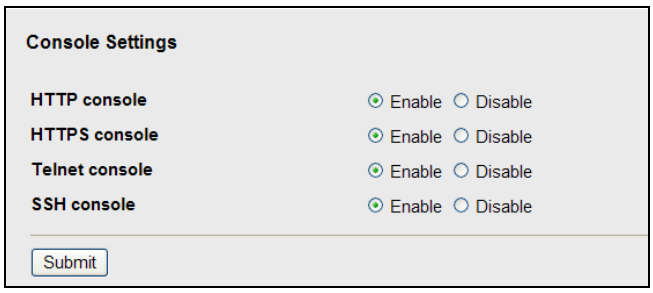


Maintenance

Maintenance functions provide the administrator with tools to manage the IE-WL-AP-BR-CL-ABG and wired/wireless networks.

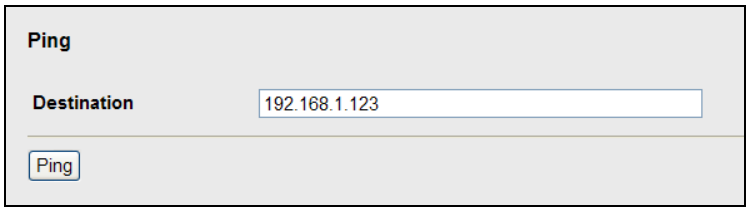
Console Settings

You can enable or disable access permission for the following consoles: HTTP, HTTPS, Telnet and SSH connections. For more security, we recommend you only allow access to the two secured consoles, HTTPS and SSH.

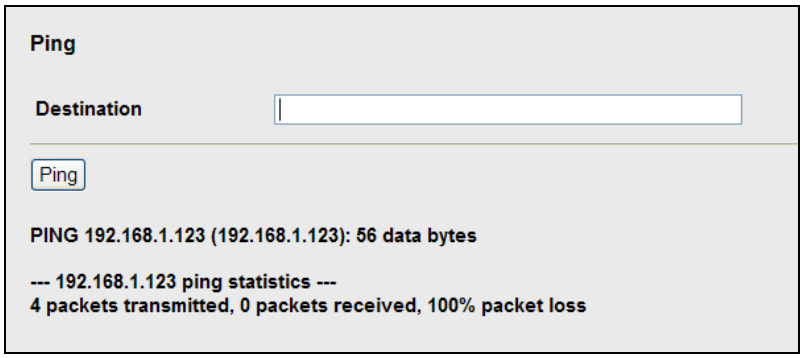


Ping

Ping helps to diagnose the integrity of wired or wireless networks. By inputting a node's IP address in the **Destination** field, you can use the **ping** command to make sure it exists and whether or not the access path is available.



If the node and access path are available, you will see that all packets were successfully transmitted with no loss. Otherwise, some, or even all, packets may get lost, as shown in the following figure.

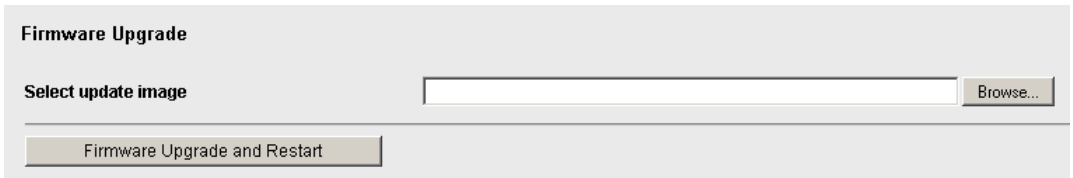


Firmware Upgrade

The IE-WL-AP-BR-CL-ABG can be enhanced with more value-added functions by installing firmware upgrades. The latest firmware is available at Weidmüller's download area on www.weidmueller.com.

Before running a firmware upgrade, make sure the IE-WL-AP-BR-CL-ABG is off-line. Click the **Browse** button to specify the firmware image file and click **Firmware Upgrade and Restart** to start the firmware upgrade. After the progress bar reaches 100%, the IE-WL-AP-BR-CL-ABG will reboot itself.

When upgrading your firmware, the IE-WL-AP-BR-CL-ABG's other functions are forbidden.



ATTENTION

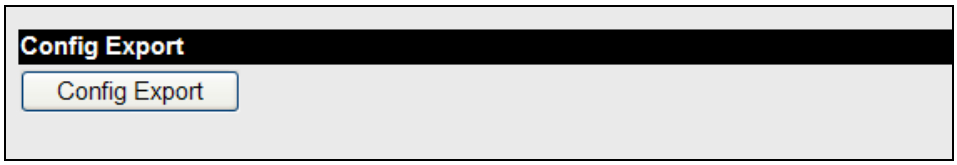
Please make sure the power source is stable when you upgrade your firmware. An unexpected power breakup may damage your IE-WL-AP-BR-CL-ABG.

Config Import Export

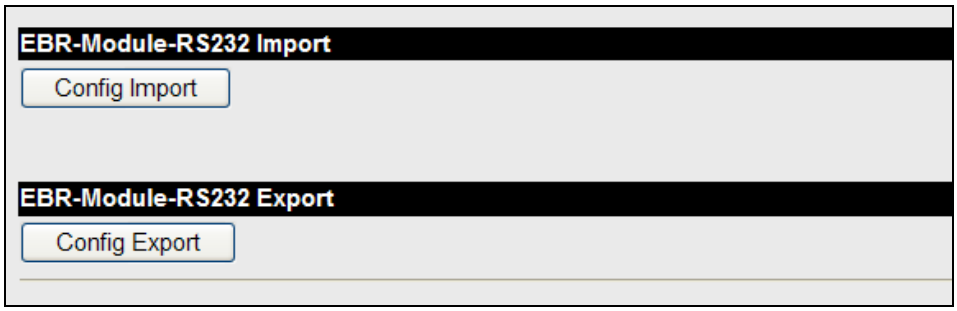
You can back up or restore the IE-WL-AP-BR-CL-ABG's configuration with **Config Import Export**.

In the **Config Import** section, click **Browse** to specify the configuration file and click **Config Import** button to begin importing the configuration.

In the **Config Export** section, click the **Config Export** button and save the configuration file onto your local storage media. The configuration file is a text file and you can view and edit it with a general text-editing tool.



You can also back up or restore the EBR-MODULE RS232 (external backup and restore module) configuration with **Config Import Export**.



To download the configuration to the IE-WL-AP-BR-CL-ABG:

i. Turn off the IE-WL-AP-BR-CL-ABG.

ii. Plug in the EBR-MODULE RS232 to the IE-WL-AP-BR-CL-ABG's RS-232 console.

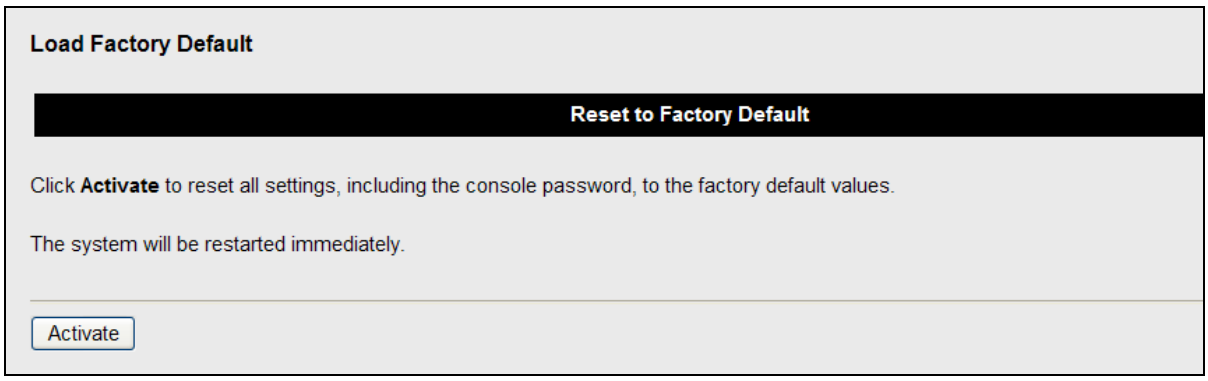
iii. Turn on IE-WL-AP-BR-CL-ABG.

iv. IE-WL-AP-BR-CL-ABG will detect EBR-MODULE RS232 during boot up, and download the configuration from the EBR-MODULE RS232 to the IE-WL-AP-BR-CL-ABG automatically. Once the configuration downloads and if configuration format is correct, the IE-WL-AP-BR-CL-ABG will emit three short beeps, and then continue the boot up.

v. Once the IE-WL-AP-BR-CL-ABG has booted up successfully, it will emit the normal two beeps, and the ready LED will turn to solid green.

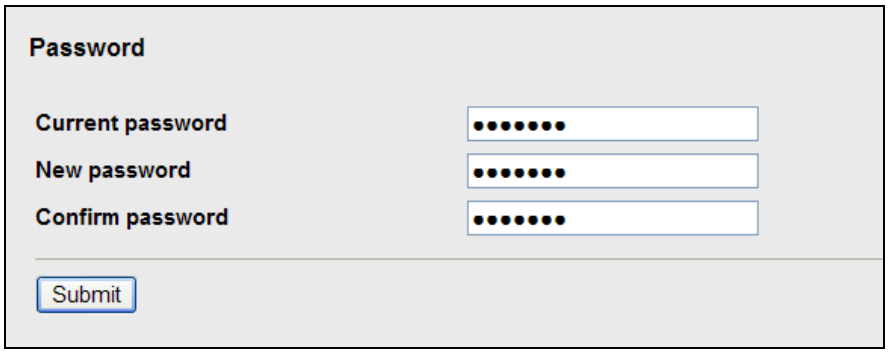
Load Factory Default

Use this function to reset the IE-WL-AP-BR-CL-ABG and roll all settings back to the factory default values. You can also reset the hardware by pressing the reset button on the top panel of the IE-WL-AP-BR-CL-ABG.


Load Factory Default
Reset to Factory Default
Click Activate to reset all settings, including the console password, to the factory default values.
The system will be restarted immediately.
Activate

Password

You can change the administration password for each of the IE-WL-AP-BR-CL-ABG's console managers by using the **Password** function. Before you set up a new password, you must input the current password and reenter the new password for confirmation. For your security, do not use the default password ***Detmold***, and remember to change the administration password regularly.



Misc. Settings

Additional settings to help you manage your IE-WL-AP-BR-CL-ABG, are available on this page.

Reset button

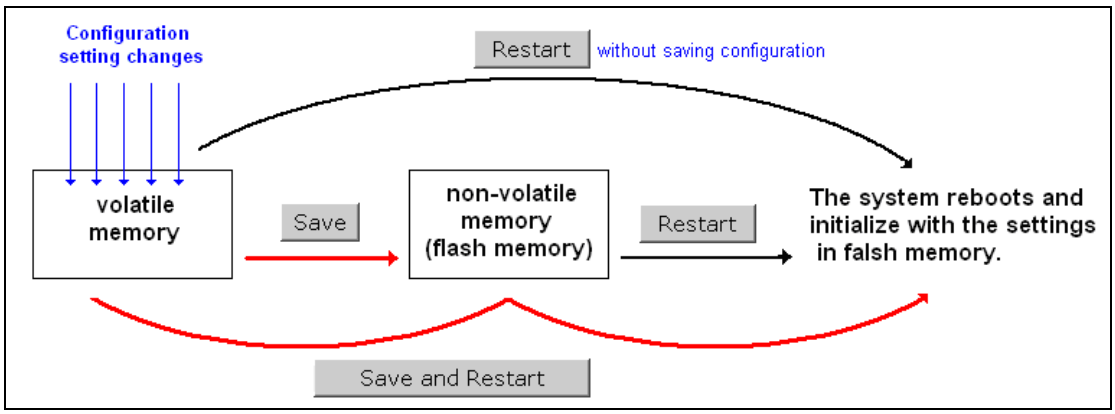
Setting	Description	Factory Default
Always enable	The IE-WL-AP-BR-CL-ABG's Reset button works normally.	Always enable
Disable after 60 sec	The IE-WL-AP-BR-CL-ABG's reset to default function will be inactive 60 seconds after the IE-WL-AP-BR-CL-ABG finishes booting up.	

Save Configuration

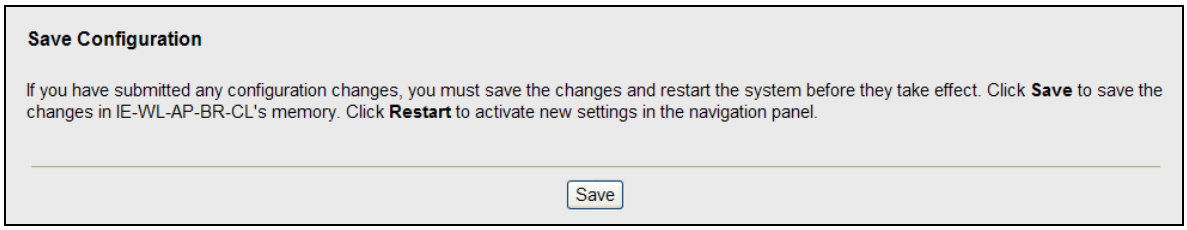
The following figure shows how the IE-WL-AP-BR-CL-ABG stores the setting changes into volatile and non-volatile memory. All data stored in volatile memory will disappear when the IE-WL-AP-BR-CL-ABG is shutdown or rebooted unless they are **y**. Because the IE-WL-AP-BR-CL-ABG starts up and initializes with the

settings stored in flash memory, all new changes must be saved to flash memory before restarting the IE-WL-AP-BR-CL-ABG.

This also means the new changes will not work unless you run either the **Save Configuration** function or the **Restart** function.



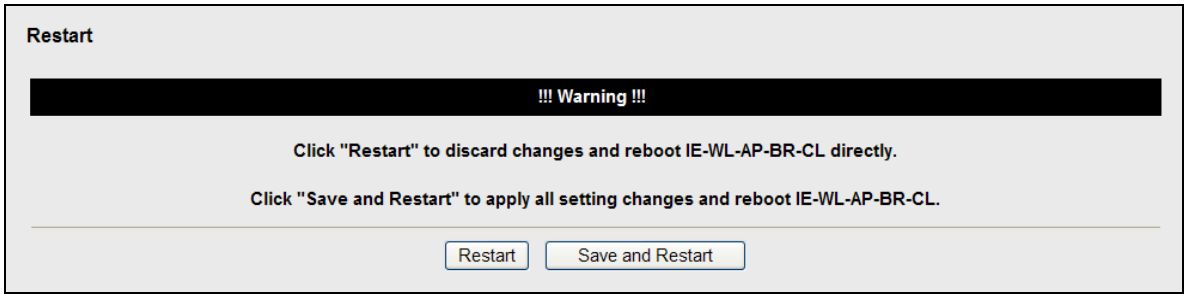
After you click on **Save Configuration** in the left menu box, the following screen will appear. Click **Save** if you wish to update the configuration settings in the flash memory at this time. Alternatively, you may choose to run other functions and put off saving the configuration until later. However, the new setting changes will remain in the non-volatile memory until you save the configurations.


Save Configuration
If you have submitted any configuration changes, you must save the changes and restart the system before they take effect. Click Save to save the changes in IE-WL-AP-BR-CL's memory. Click Restart to activate new settings in the navigation panel.
Save

Restart

If you submitted configuration changes, you will find a blinking string in the upper right corner of the screen. After making all your changes, click the **Restart** function in the left menu box. One of two different screens will appear.

If you made changes recently but did not save, you will be given two options. Clicking the **Restart** button here will reboot the IE-WL-AP-BR-CL-ABG directly, and all setting changes will be ignored. Clicking the **Save and Restart** button will apply all setting changes and then reboot the IE-WL-AP-BR-CL-ABG.

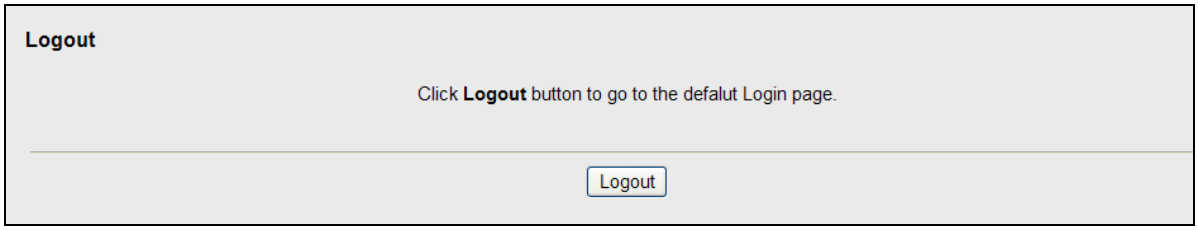

Restart
!!! Warning !!!
Click "Restart" to discard changes and reboot IE-WL-AP-BR-CL directly.
Click "Save and Restart" to apply all setting changes and reboot IE-WL-AP-BR-CL.
Restart
Save and Restart

If you run the **Restart** function without changing any configurations or saving all your changes, you will see just one **Restart** button on your screen.

You will not be able to run any of the IE-WL-AP-BR-CL-ABG's functions while the system is rebooting.

Logout

Logout helps users disconnect the current HTTP or HTTPS session and go to the Login page. For security reasons, we recommend you logout before quitting the console manager.



4

Software Installation and Configuration

The following topics are covered in this chapter:

- **WLAN Administration Tool**
  - Installing WLAN Administration Tool
  - Configuring WLAN Administration Tool

WLAN Administration Tool

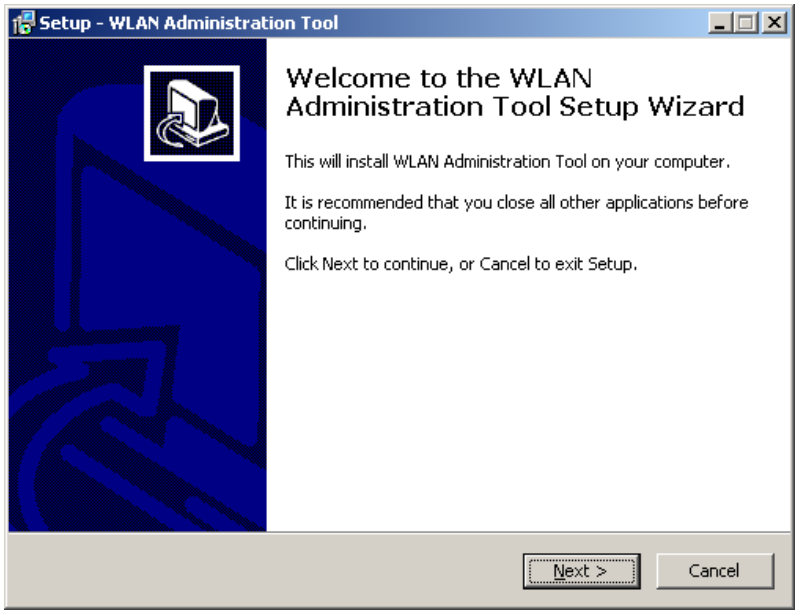
NOTE You may download the WLAN Administration Tool from the Weidmüller website using the following path:

1. Open www.weidmueller.com/Downloads
2. Select page “Software”
3. Select page “Industrial Ethernet”
4. Select category **“**Industrial Wireless (Firmware and Software for IE-WL-AP-BR-CL-ABG)**”**
5. Download “WLAN Administration Tool”

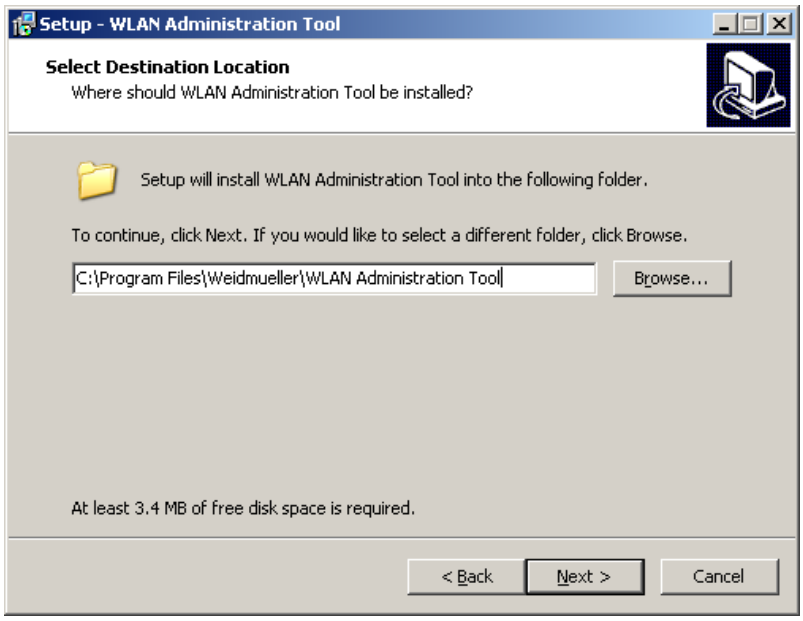
Installing WLAN Administration Tool

For example, if the file was placed on the Windows desktop, it should appear as follows. Simply double click on the icon to run the program.

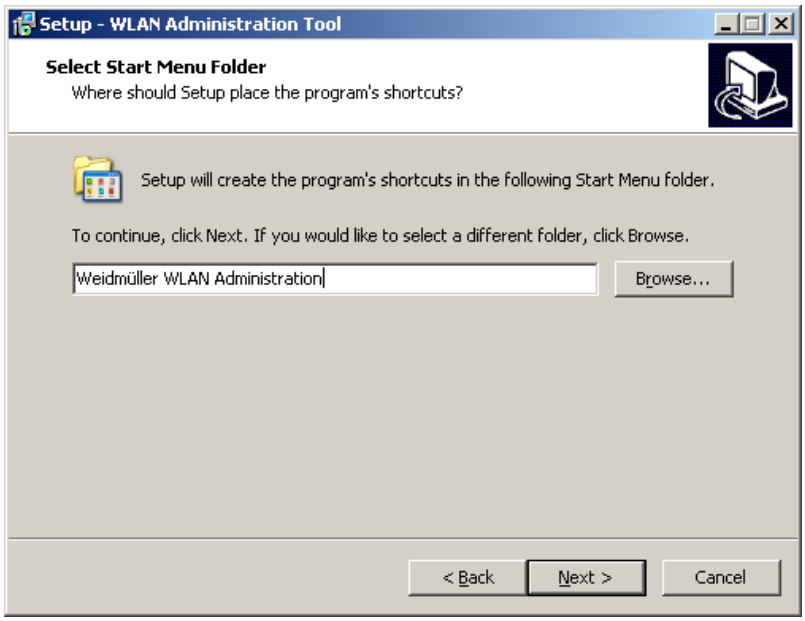
1. Click **Next** when the **Welcome** screen opens to proceed with the installation.


Setup - WLAN Administration Tool
Welcome to the WLAN Administration Tool Setup Wizard
This will install WLAN Administration Tool on your computer.
It is recommended that you close all other applications before continuing.
Click Next to continue, or Cancel to exit Setup.
Next >
Cancel

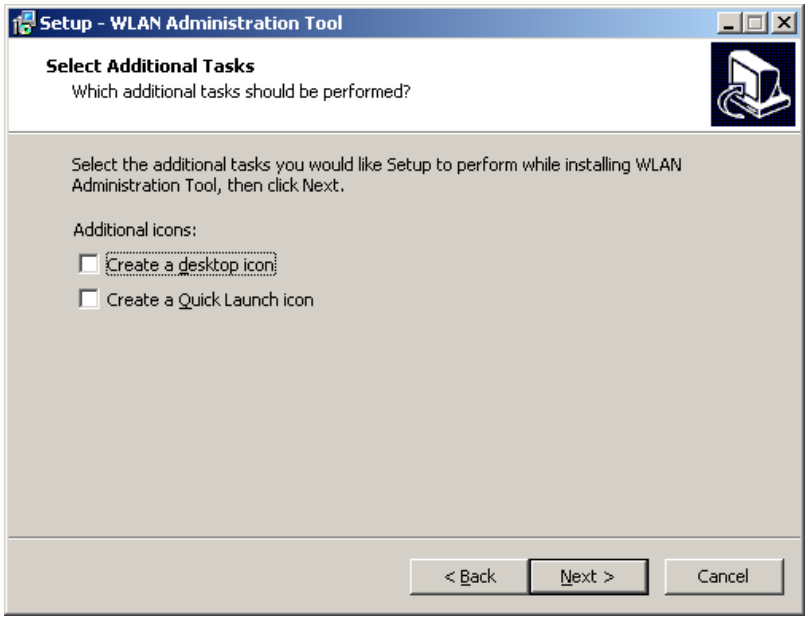
2. Click **Next** to install program files to the default directory, or click **Browse** to select an alternate location.


Setup - WLAN Administration Tool
Select Destination Location
Where should WLAN Administration Tool be installed?
Setup will install WLAN Administration Tool into the following folder.
To continue, click Next. If you would like to select a different folder, click Browse.
C:\Program Files\Weidmueller\WLAN Administration Tool
Browse...
At least 3.4 MB of free disk space is required.
< Back
Next >
Cancel

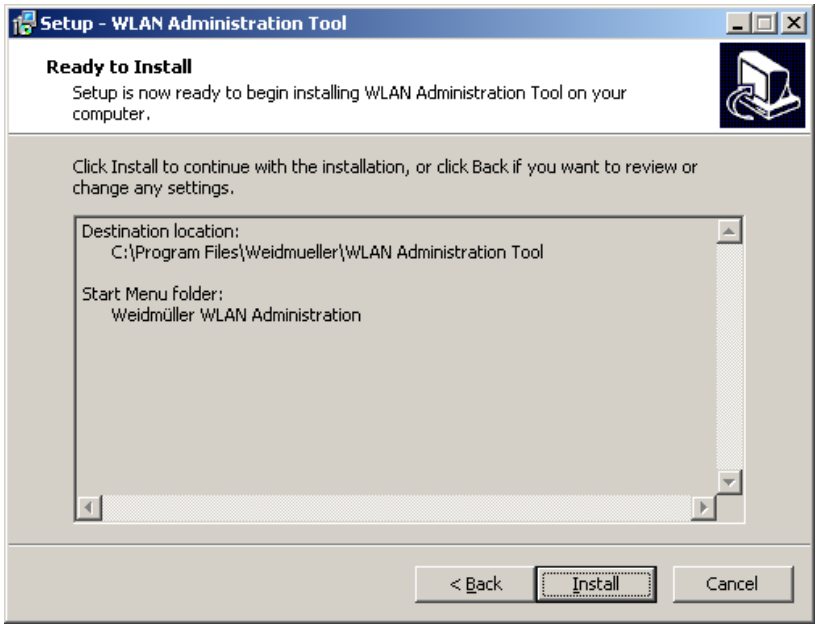
3. Click **Next** to create the program's shortcut files to the default directory, or click **Browse** to select an alternate location.


Setup - WLAN Administration Tool
Select Start Menu Folder
Where should Setup place the program's shortcuts?
Setup will create the program's shortcuts in the following Start Menu folder.
To continue, click Next. If you would like to select a different folder, click Browse.
Weidmüller WLAN Administration
Browse...
< Back
Next >
Cancel

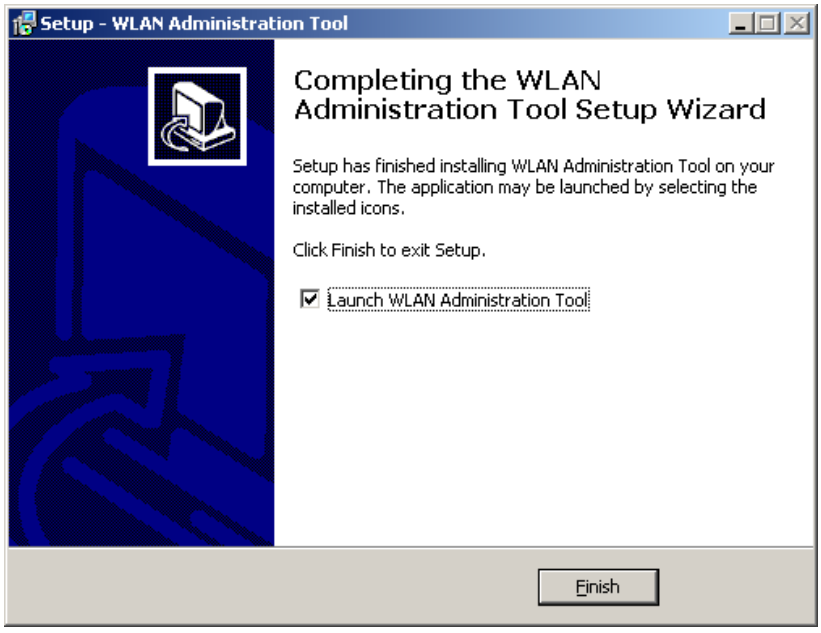
4. Click **Next** to select additional tasks.


Setup - WLAN Administration Tool
Select Additional Tasks
Which additional tasks should be performed?
Select the additional tasks you would like Setup to perform while installing WLAN Administration Tool, then click Next.
Additional icons:
Create a desktop icon
Create a Quick Launch icon
< Back
Next >
Cancel

5. Click **Next** to proceed with the installation. The installer then displays a summary of the installation options.


Setup - WLAN Administration Tool
Ready to Install
Setup is now ready to begin installing WLAN Administration Tool on your computer.
Click Install to continue with the installation, or click Back if you want to review or change any settings.
Destination location:
C:\Program Files\Weidmueller\WLAN Administration Tool
Start Menu folder:
Weidmüller WLAN Administration
< Back
Install
Cancel

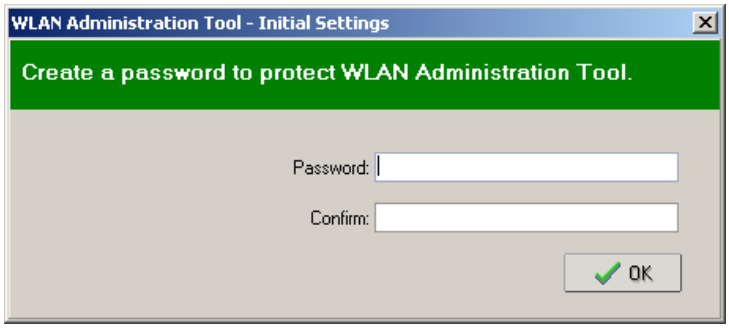
6. Click **Install** to begin the installation. The setup window will report the progress of the installation. To change the installation settings, click **Back** and navigate to the previous screen.
7. Click **Finish** to complete the installation of WLAN Administration Tool.


Setup - WLAN Administration Tool
Completing the WLAN Administration Tool Setup Wizard
Setup has finished installing WLAN Administration Tool on your computer. The application may be launched by selecting the installed icons.
Click Finish to exit Setup.
Launch WLAN Administration Tool
Finish

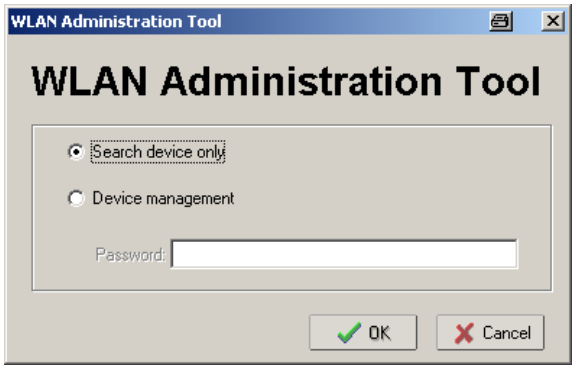
Configuring WLAN Administration Tool

The Broadcast Search function is used to locate all IE-WL-AP-BR-CL-ABG APs that are connected to the same LAN as your computer. After locating an IE-WL-AP-BR-CL-ABG, you will be able to change its IP address. Since the Broadcast Search function searches by TCP packet and not IP address, it doesn't matter if the IE-WL-AP-BR-CL-ABG is configured as an AP or Client. In either case, APs and Clients connected to the LAN will be located, regardless of whether or not they are part of the same subnet as the host.

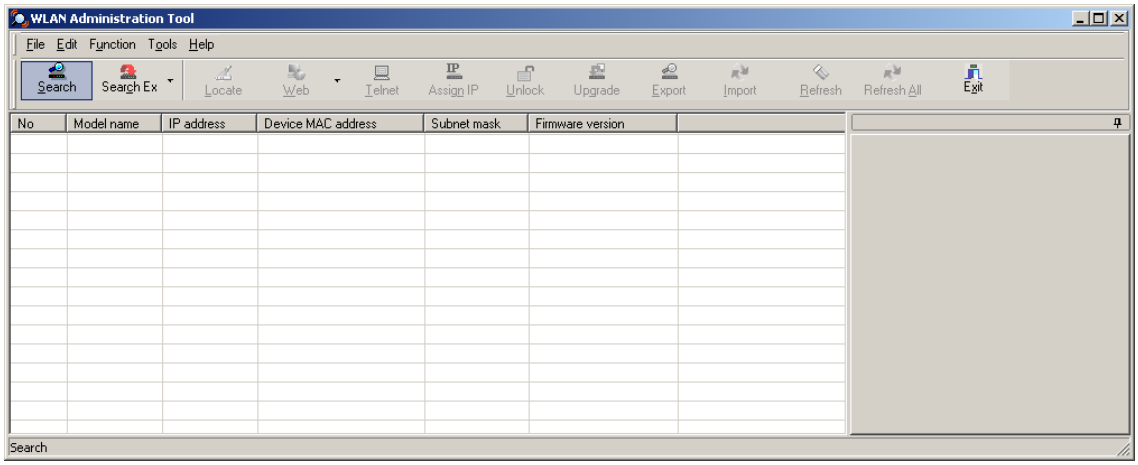
1. Start the WLAN Administration Tool program. After the first start of the WLAN Administration Tool the following window appears. There you have the possibility to set a password for access to the "device management function"



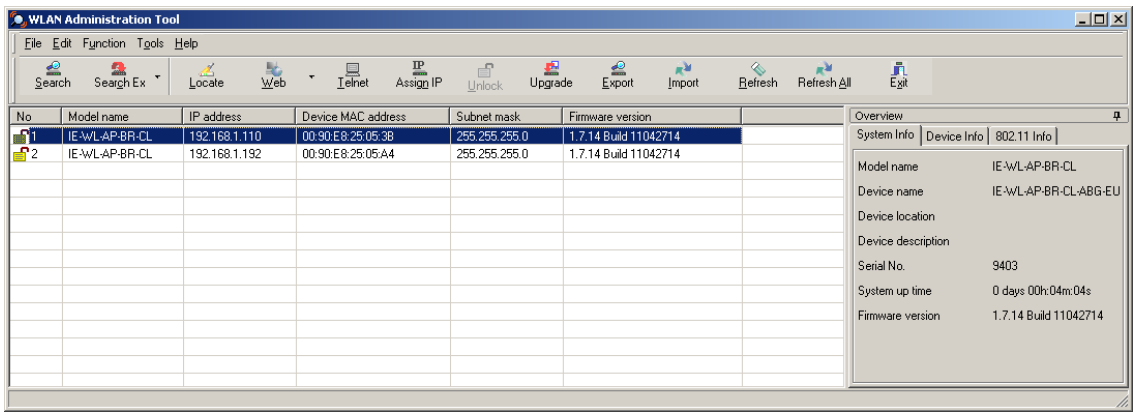
2. When the Login page appears, select the "Search Device only" option to search for IE-WL-AP-BR-CL-ABGs and to view each IE-WL-AP-BR-CL-ABG's configuration. Select the "Device management" option to assign IPs, upgrade firmware, and locate devices.



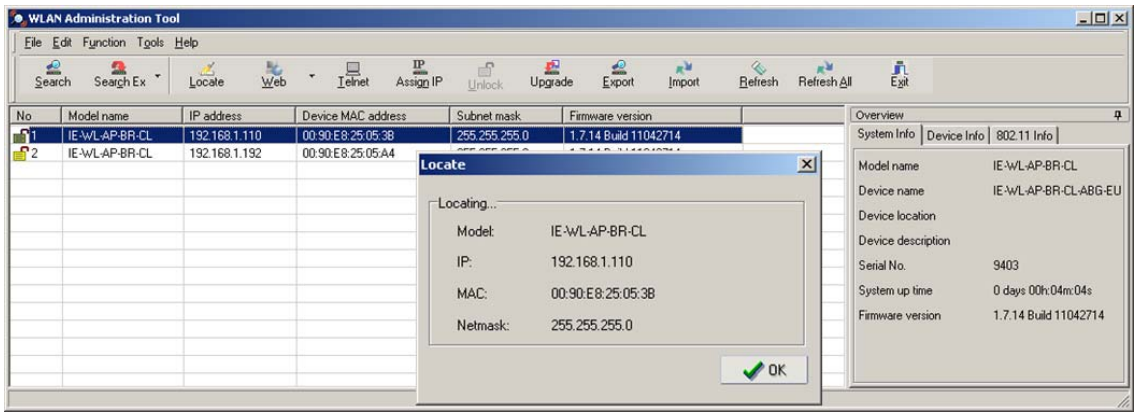
3. The WLAN Administration Tool will start automatically. Then click the **Search** icon.



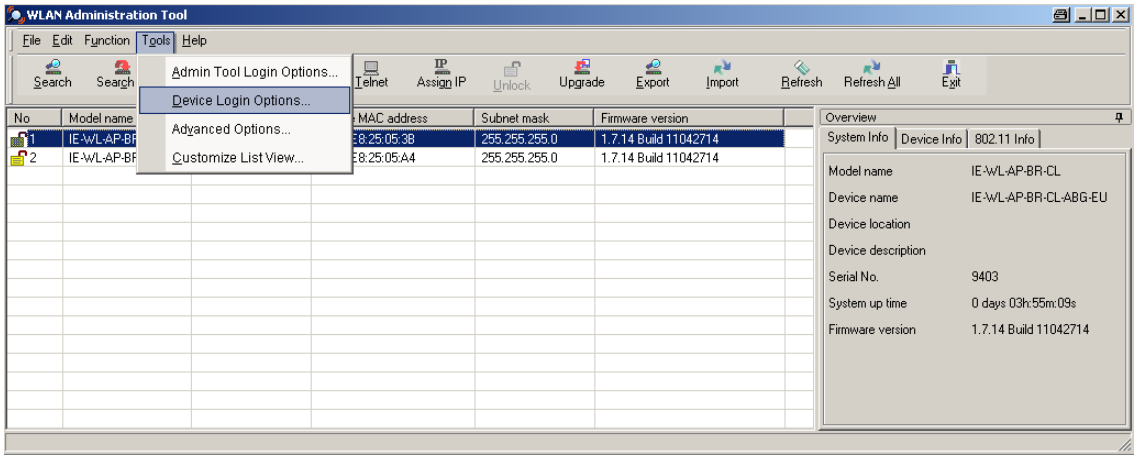
4. The "Searching" window indicates the progress of the search. When the search is complete, all IE-WL-AP-BR-CL-ABGs that were located will be displayed in the WLAN Administration Tool window.



5. Click **Locate** to cause the selected device to beep.


WLAN Administration Tool
File Edit Function Tools Help
Search Search Ex Locate Web Telnet Assign IP Unlock Upgrade Export Import Refresh Refresh All Exit
No Model name IP address Device MAC address Subnet mask Firmware version
1 IE-WL-AP-BR-CL 192.168.1.110 00:90:E8:25:05:3B 255.255.255.0 1.7.14 Build 11042714
2 IE-WL-AP-BR-CL 192.168.1.192 00:90:E8:25:05:A4
Locate
Locating...
Model: IE-WL-AP-BR-CL
IP: 192.168.1.110
MAC: 00:90:E8:25:05:3B
Netmask: 255.255.255.0
OK
Overview
System Info Device Info 802.11 Info
Model name IE-WL-AP-BR-CL
Device name IE-WL-AP-BR-CL-ABG-EU
Device location
Device description
Serial No. 9403
System up time 0 days 00h:04m:04s
Firmware version 1.7.14 Build 11042714

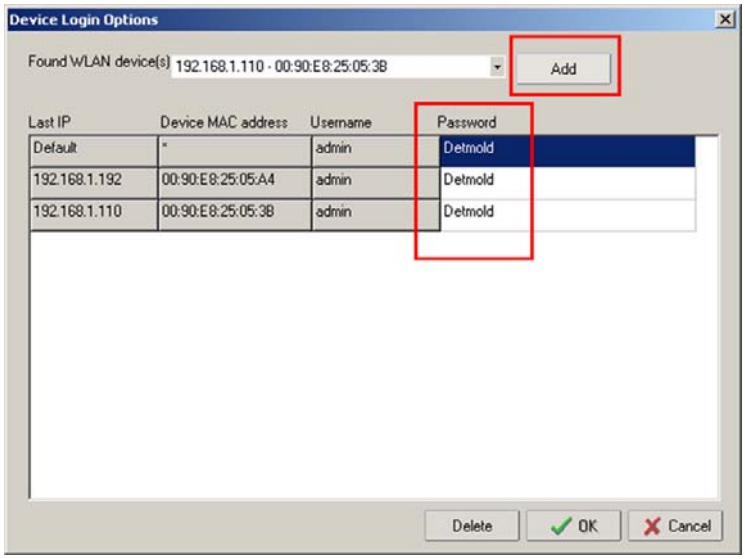
6. Make sure your IE-WL-AP-BR-CL-ABG is **unlocked** before using the Administration Tool's icons setting. The IE-WL-AP-BR-CL-ABG will unlock automatically if the password is set to the default. Otherwise you must enter the new password manually.
7. Go to **Tools → Device Login Options** to manage and unlock additional IE-WL-AP-BR-CL-ABGs.


WLAN Administration Tool
File Edit Function Tools Help
Admin Tool Login Options...
Device Login Options...
Advanced Options...
Customize List View...
Search Telnet Assign IP Unlock Upgrade Export Import Refresh Refresh All Exit
No Model name Subnet mask Firmware version
1 255.255.255.0 1.7.14 Build 11042714
2 255.255.255.0 1.7.14 Build 11042714
Overview
System Info Device Info 802.11 Info
Model name IE-WL-AP-BR-CL
Device name IE-WL-AP-BR-CL-ABG-EU
Device location
Device description
Serial No. 9403
System up time 0 days 03h:55m:09s
Firmware version 1.7.14 Build 11042714

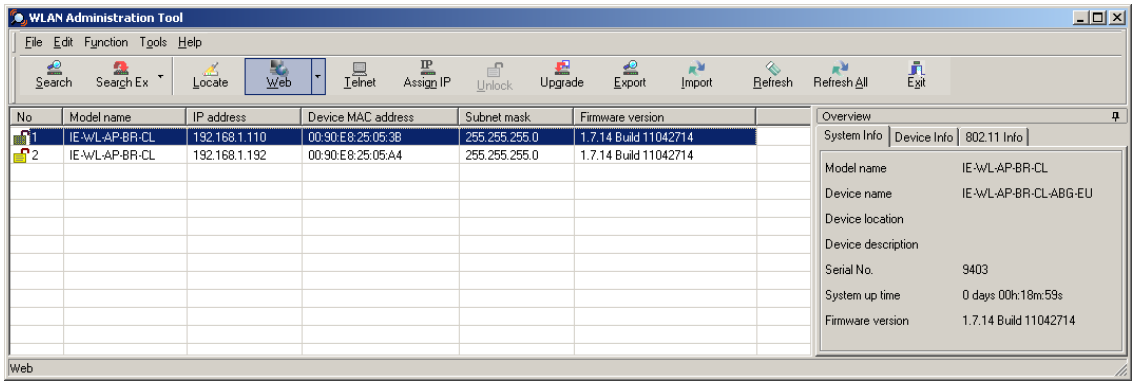
8. Use the scroll down list to select the MAC addresses of those IE-WL-AP-BR-CL-ABGs you would like to manage, and then click **Add**. Key in the password for the IE-WL-AP-BR-CL-ABG device and then click **OK** to save. If you return to the search page and search for the IE-WL-AP-BR-CL-ABG again, you will find that the IE-WL-AP-BR-CL-ABG will unlock automatically.

ATTENTION

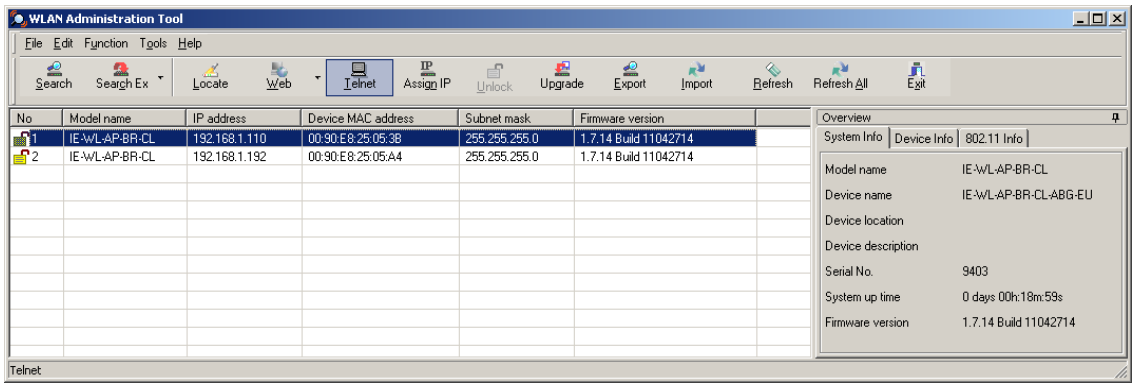
For security purposes, we suggest you can change the WLAN Administration Tool login password instead of using the default.


Device Login Options
Found WLAN device(s) 192.168.1.110 - 00:90:E8:25:05:3B
Add
Last IP Device MAC address Username Password
Default * admin Detmold
192.168.1.192 00:90:E8:25:05:A4 admin Detmold
192.168.1.110 00:90:E8:25:05:3B admin Detmold
Delete OK Cancel

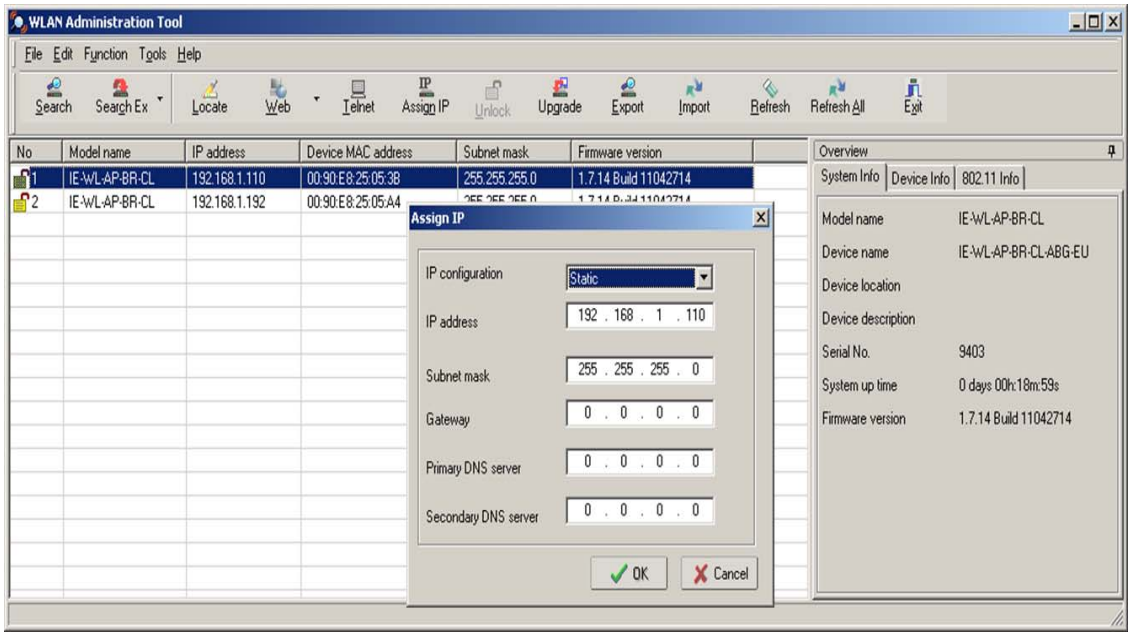
To modify the configuration of the highlighted IE-WL-AP-BR-CL-ABG, click on the Web icon to open the web console. This will take you to the web console, where you can make all configuration changes. Refer to Chapter 3, "Using the Web Console," for information on how to use the web console.


WLAN Administration Tool
File Edit Function Tools Help
Search Search Ex Locate Web Telnet Assign IP Unlock Upgrade Export Import Refresh Refresh All Exit
No Model name IP address Device MAC address Subnet mask Firmware version
1 IE-WL-AP-BR-CL 192.168.1.110 00:90:E8:25:05:3B 255.255.255.0 1.7.14 Build 11042714
2 IE-WL-AP-BR-CL 192.168.1.192 00:90:E8:25:05:A4 255.255.255.0 1.7.14 Build 11042714
Overview
System Info Device Info 802.11 Info
Model name IE-WL-AP-BR-CL
Device name IE-WL-AP-BR-CL-ABG-EU
Device location
Device description
Serial No. 9403
System up time 0 days 00h:18m:59s
Firmware version 1.7.14 Build 11042714
Web

Click on **Telnet** if you would like to use telnet to configure your IE-WL-AP-BR-CL-ABGs.


WLAN Administration Tool
File Edit Function Tools Help
Search Search Ex Locate Web Telnet Assign IP Unlock Upgrade Export Import Refresh Refresh All Exit
No Model name IP address Device MAC address Subnet mask Firmware version
1 IE-WL-AP-BR-CL 192.168.1.110 00:90:E8:25:05:3B 255.255.255.0 1.7.14 Build 11042714
2 IE-WL-AP-BR-CL 192.168.1.192 00:90:E8:25:05:A4 255.255.255.0 1.7.14 Build 11042714
Overview
System Info Device Info 802.11 Info
Model name IE-WL-AP-BR-CL
Device name IE-WL-AP-BR-CL-ABG-EU
Device location
Device description
Serial No. 9403
System up time 0 days 00h:18m:59s
Firmware version 1.7.14 Build 11042714
Telnet

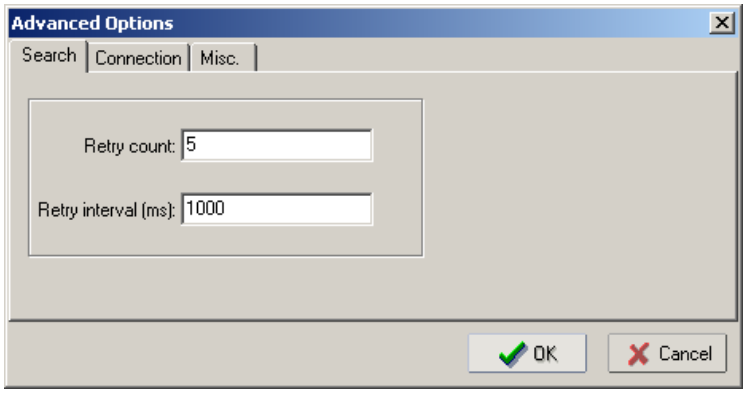
Click **Assign IP** to change the IP setting.


WLAN Administration Tool
File Edit Function Tools Help
Search Search Ex Locate Web Telnet Assign IP Unlock Upgrade Export Import Refresh Refresh All Exit
No Model name IP address Device MAC address Subnet mask Firmware version
1 IE-WL-AP-BR-CL 192.168.1.110 00:90:E8:25:05:3B 255.255.255.0 1.7.14 Build 11042714
2 IE-WL-AP-BR-CL 192.168.1.192 00:90:E8:25:05:A4
Assign IP
IP configuration Static
IP address 192 . 168 . 1 . 110
Subnet mask 255 . 255 . 255 . 0
Gateway 0 . 0 . 0 . 0
Primary DNS server 0 . 0 . 0 . 0
Secondary DNS server 0 . 0 . 0 . 0
OK Cancel
Overview
System Info Device Info 802.11 Info
Model name IE-WL-AP-BR-CL
Device name IE-WL-AP-BR-CL-ABG-EU
Device location
Device description
Serial No. 9403
System up time 0 days 00h:18m:59s
Firmware version 1.7.14 Build 11042714

The three advanced options—**Search**, **Connection**, and **Miscellaneous**—are explained below:

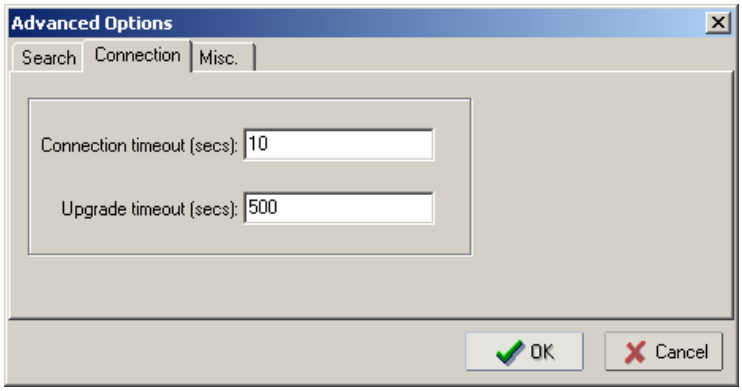
Search

- **Retry count (default=5):** Indicates how many times the search will be retried automatically.
- **Retry interval (ms):** The time lapsed between retries.



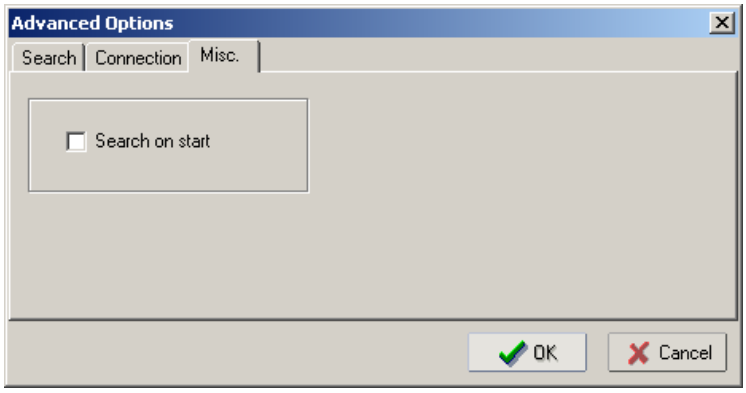
Connection

- **Connection timeout (secs):** Use this option to set the waiting time for the **Default Login**, **Locate**, **Assign IP**, **Upload Firmware**, and **Unlock** to complete.
- **Upgrade timeout (secs):** Use this option to set the waiting time for the connection to disconnect while the firmware is upgrading. Use this option to set the waiting time for the Firmware to write to flash.



Misc.

Search on start: Checkmark this box if you would like the search function to start searching for devices after you log in to the WLAN Administration Tool.



5

Other Console Considerations

This chapter explains how to access the IE-WL-AP-BR-CL-ABG for the first time. In addition to HTTP access, there are four ways to access IE-WL-AP-BR-CL-ABG: serial console, Telnet console, SSH console, and HTTPS console. The serial console connection method, which requires using a short serial cable to connect the IE-WL-AP-BR-CL-ABG to a PC's COM port, can be used if you do not know the IE-WL-AP-BR-CL-ABG's IP address. The other consoles can be used to access the IE-WL-AP-BR-CL-ABG over an Ethernet LAN, or over the Internet.

The following topics are covered in this chapter:

- **RS-232 Console Configuration (115200, None, 8, 1, VT100)**
- **Configuration by Telnet and SSH Consoles**
- **Configuration by Web Browser with HTTPS/SSL**
- **Disabling Telnet and Browser Access**

RS-232 Console Configuration (115200, None, 8, 1, VT100)

The serial console connection method, which requires using a short serial cable to connect the IE-WL-AP-BR-CL-ABG to a PC's COM port, can be used if you do not know the IE-WL-AP-BR-CL-ABG's IP address. It is also convenient to use serial console configurations when you cannot access the IE-WL-AP-BR-CL-ABG over Ethernet LAN, such as in the case of LAN cable disconnections or broadcast storming over the LAN.

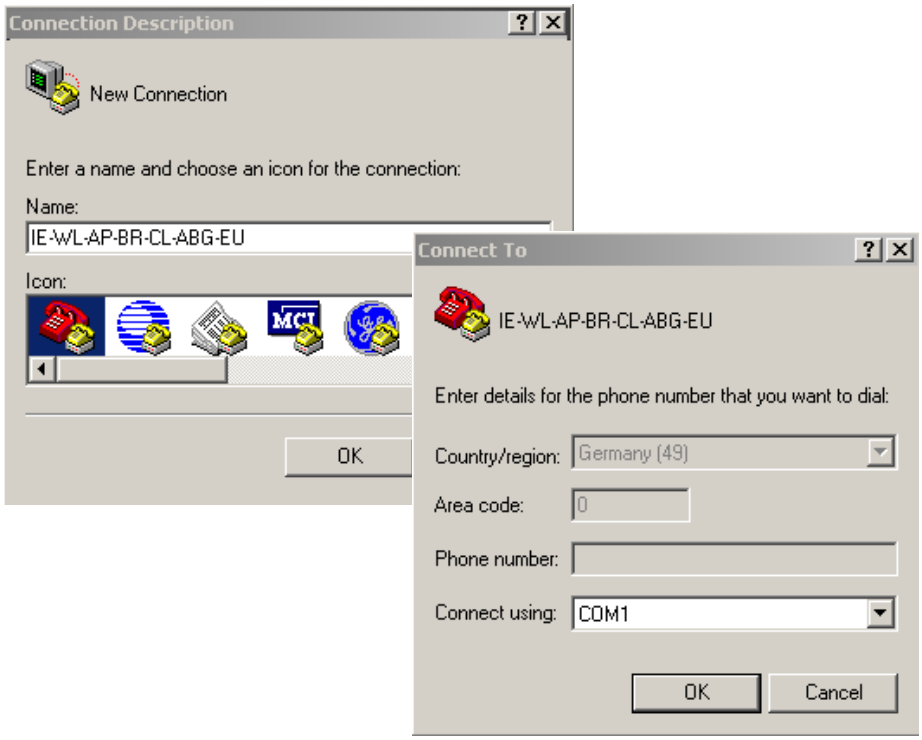
ATTENTION

Do not use the RS-232 console manager when the IE-WL-AP-BR-CL-ABG is powered at reversed voltage (ex. -48VDC), even though reverse voltage protection is supported.

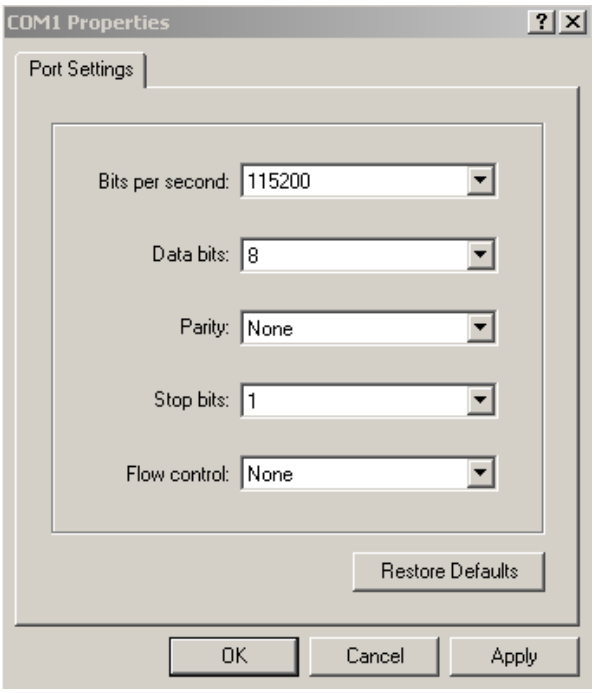
NOTE We recommend using Hyper Terminal Program, which is already installed under Windows XP operating system.

Before running Hyper Terminal Program, use an RJ45 to DB9-F (or RJ45 to DB25-F) cable to connect the IE-WL-AP-BR-CL-ABG's RS-232 console port to your PC's COM port (generally COM1 or COM2, depending on how your system is set up). After starting Hyper Terminal Program, take the following steps to access the RS-232 console configuration.

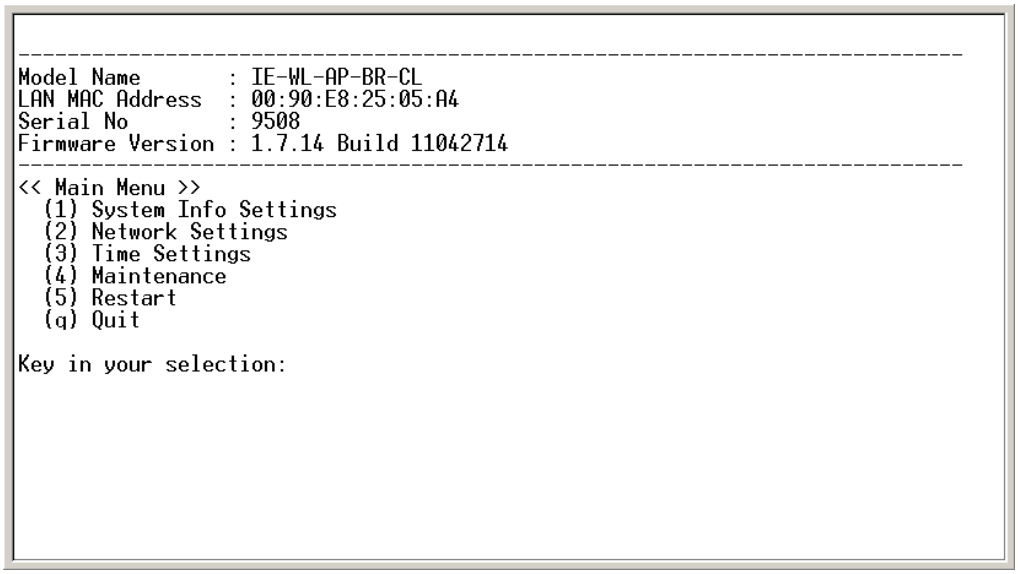
1. From the Windows desktop, click Start –> Programs -> Accessories -> Communications -> Hyper Terminal.
2. Start Hyper Terminal and enter a name of your choice for the new connection. Select the appropriate COM port for console connection in the "New Connection" window.



3. Select following Communication Parameter for the console connection:
   115200 for Baud Rate, **8** for Data Bits, **None** for Parity, and **1** for Stop Bits and None for Flow control. Click on **OK** to continue.



4. The Console login screen will appear. Enter **t**he default login "**admin**" and then enter the default **Console Password** "**Detmold**" (this is the same as the Web Browser password) and then press **Enter**.



5. The IE-WL-AP-BR-CL-ABG´s Main Menu will be displayed

6. After entering the Main Menu, use the shown keys to move to select options.

ATTENTION

If you unplug the RS-232 cable or trigger **DTR**, a disconnection event will be evoked to enforce logout for network security. You will need to log in again to resume operation.

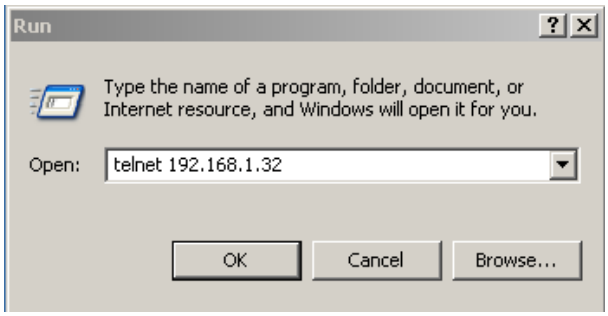
Configuration by Telnet and SSH Consoles

You may use Telnet or SSH client to access the IE-WL-AP-BR-CL-ABG and manage the console over a network. To access the IE-WL-AP-BR-CL-ABG's functions over the network from a PC host that is connected to the same LAN as the IE-WL-AP-BR-CL-ABG, you need to make sure that the PC host and the IE-WL-AP-BR-CL-ABG are on the same logical subnet. To do this, check your PC host's IP address and subnet mask.

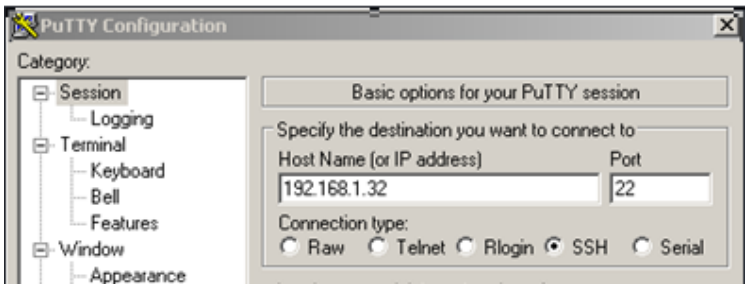
NOTE The IE-WL-AP-BR-CL-ABG's default IP address is **192.168.1.110** and the default subnet mask is **255.255.255.0** (for a Class C network). If you do not set these values properly, please check the network settings of your PC host and then change the IP address to 192.168.1.xxx and subnet mask to 255.255.255.0.

Follow the steps below to access the console utility via Telnet or SSH client.

1. From Windows Desktop, run **Start → Run**, and then use Telnet to access the IE-WL-AP-BR-CL-ABG's IP address from the Windows Run window (you may also issue the telnet command from the MS-DOS prompt).



2. When using SSH client (ex. PuTTY), please run the client program (ex. putty.exe) and then input the IE-WL-AP-BR-CL-ABG's IP address, specifying **22** for the SSH connection port.



3. The Console login screen will appear. Please refer to the previous paragraph "RS-232 Console Configuration" and for login and administration.

Configuration by Web Browser with HTTPS/SSL

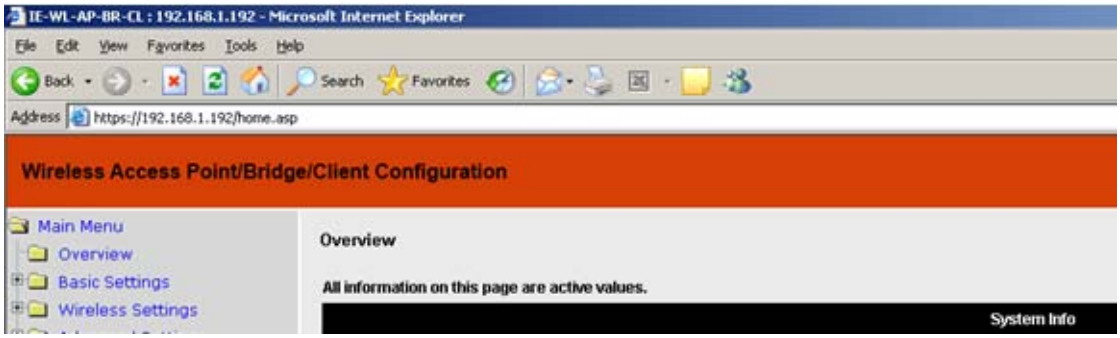
To secure your HTTP access, the IE-WL-AP-BR-CL-ABG supports HTTPS/SSL encryption for all HTTP traffic. Perform the following steps to access the IE-WL-AP-BR-CL-ABG's web browser interface via HTTPS/SSL.

1. Open your web browser and type https://< IE-WL-AP-BR-CL-ABG's IP address> in the address field. Press **Enter** to establish the connection.

2. Warning messages will pop out to warn users that the security certificate was issued by a company they have not chosen to trust.

Security Alert
Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.
The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.
The security certificate date is valid.
The security certificate has a valid name matching the name of the page you are trying to view.
Do you want to proceed?
Yes
No
View Certificate

3. Select **Yes** to accept the certificate and then enter the IE-WL-AP-BR-CL-ABG's web browser interface secured via HTTPS/SSL. (You can see the protocol in URL is **https**.) Then you can use the menu tree on the left side of the window to open the function pages to access each of IE-WL-AP-BR-CL-ABG's functions.



Disabling Telnet and Browser Access

If you are connecting the IE-WL-AP-BR-CL-ABG to a public network but do not intend to use its management functions over the network, then we suggest disabling both Telnet Console and Web Configuration. Please run **Maintenance → Console Settings** to disable them, as shown in the following figure.

A

References

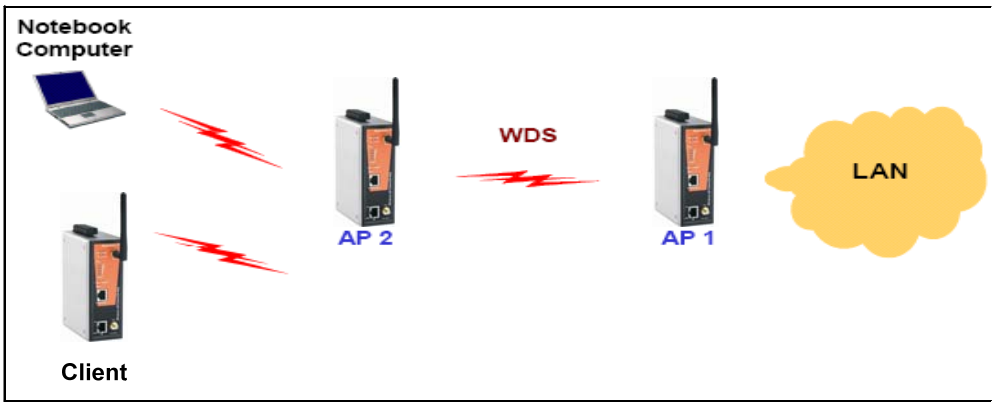
This chapter provides more detailed information about wireless-related technologies. The information in this chapter can help you administer your IE-WL-AP-BR-CL-ABGs and plan your industrial wireless network better.

The following topics are covered in this appendix:

- **Wireless Distribution System (WDS)**
- **Beacon**
- **DTIM**
- **Fragment**
- **RTS Threshold**
- **STP and RSTP**
  - The STP/RSTP Concept
  - Differences between RSTP and STP

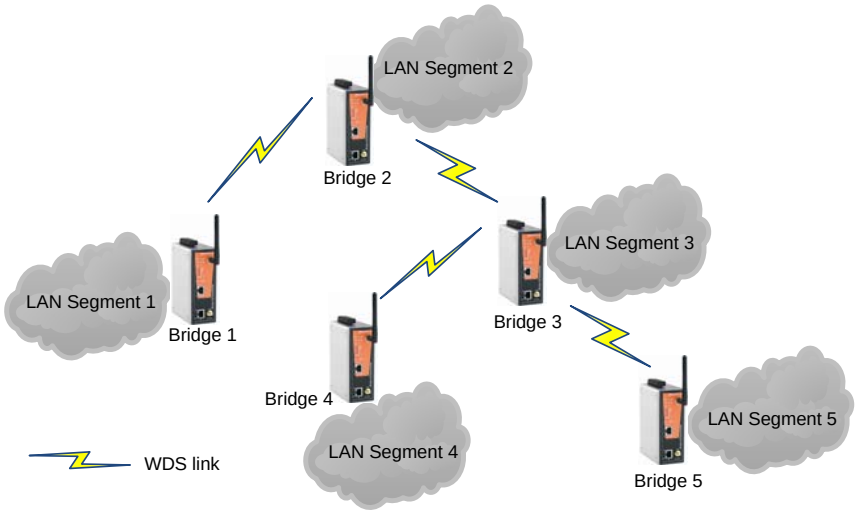
Wireless Distribution System (WDS)

Traditionally, APs are connected via Ethernet LAN ports. By using a Wireless Distribution System (WDS), APs can communicate with one another wirelessly. For example, AP 2 acts as an access point for the notebook computers or other IEEE802.11-enabled clients, and forwards packets sent from the notebook computers to AP 1 through WDS. Then, AP 1 forwards the packets to the Ethernet LAN. Packets destined for the notebook computers follow a reverse path from the Ethernet LAN through the APs to the notebook computers. In this way, AP 2 acts as an "AP repeater."



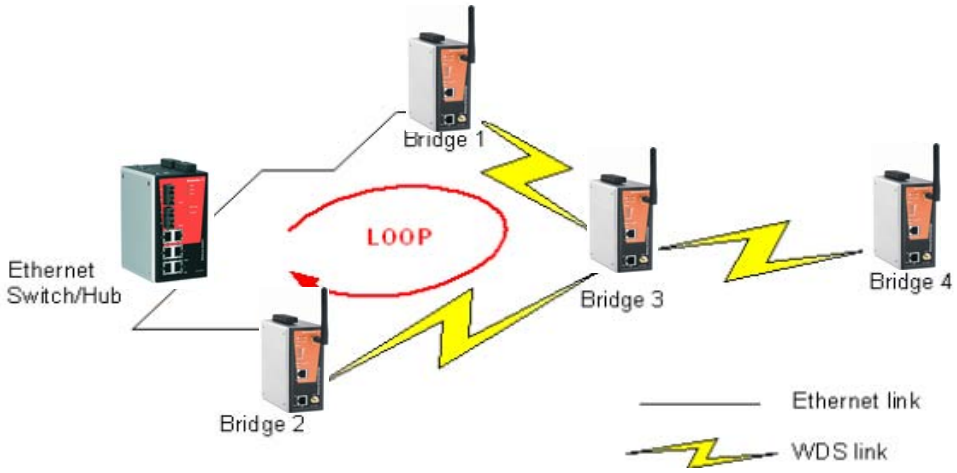
By using WDS, two or more LAN segments can be connected wirelessly. As illustrated in the below figure, a pair of wireless LAN-to-LAN bridges is used to connect two LAN segments. Since the AP is WDS-enabled, it can be used as a wireless bridge.

It is a good idea to plan your wireless network by drawing a diagram so that you know how each IE-WL-AP-BR-CL-ABG is connected to other peer APs or wireless bridges by WDS, and how bridges are connected to other peer bridges by WDS. See the following figure for an example of a network-planning diagram.



ATTENTION

Be sure to eliminate loops from networks that consist of wireless bridges, Ethernet switches, Ethernet links, and WDS links. If any loops exist, packets will circle around the loops and network performance will be seriously degraded. The following figure shows a network topology containing a loop.



Beacon

A beacon is a packet broadcast by the AP to keep the network synchronized. A beacon includes the wireless LAN service area, the AP address, the Broadcast destination address, a time stamp, Delivery Traffic Indicator Maps (DTIM), and the Traffic Indicator Message (TIM). Beacon Interval indicates the frequency interval of AP.

DTIM

Delivery Traffic Indication Map (DTIM) is contained in beacon frames. It is used to indicate that broadcast and multicast frames buffered by the AP will be delivered shortly. Lower settings result in more efficient networking, while preventing your PC from dropping into power-saving sleep mode. Higher settings allow your PC to enter sleep mode, thus saving power.

Fragment

A lower setting means smaller packets, which will create more packets for each transmission. If you have decreased this value and experience high packet error rates, you can increase it again, but it will likely decrease overall network performance. Only minor modifications of this value are recommended.

RTS Threshold

RTS Threshold (256-2346) – This setting determines how large a packet can be before the Access Point coordinates transmission and reception to ensure efficient communication. This value should remain at its default setting of 2,346. When you encounter inconsistent data flow, only minor modifications are recommended.

STP and RSTP

The STP / RSTP Concept

Spanning Tree Protocol (STP) was designed to help reduce link failures in a network, and provide protection from loops. Networks that have a complicated architecture are prone to broadcast storms caused by unintended loops in the network. The STP protocol is part of the IEEE802.1D standard, 1998 Edition bridge specification.

Rapid Spanning Tree Protocol (RSTP) implements the Spanning Tree Algorithm and Protocol defined by IEEE802.1w-2001 standard. RSTP provides the following benefits:

- The topology of a bridged network will be determined much more quickly compared to STP.
- RSTP is backward compatible with STP, making it relatively easy to deploy. For example:
  - Defaults to sending 802.1D-style BPDUs if packets with this format are received.
  - STP (802.1D) and RSTP (802.1w) can operate on the LAN ports and WLAN ports (AP and WDS1-WDS8) of the same IE-WL-AP-BR-CL-ABG.

This feature is particularly helpful when the IE-WL-AP-BR-CL-ABG connects to older equipment, such as legacy switches.

Differences between RSTP and STP

RSTP is similar to STP, but includes additional information in the BPDUs that allow each bridge to confirm that it has taken action to prevent loops from forming when it decides to enable a link to a neighboring bridge. Adjacent bridges connected via point-to-point links will be able to enable a link without waiting to ensure that all other bridges in the network have had time to react to the change. The main benefit of RSTP is that the configuration decision is made locally rather than network-wide, allowing RSTP to carry out automatic configuration and restore a link faster than STP.

B

Supporting Information

This chapter presents additional information about this manual and product. You can also learn how to contact Weidmüller for technical support.

The following topics are covered in this appendix:

- **About This User's Manual**
- **DoC (Declaration of Conformity)**
  - Federal Communication Commission Interference Statement
  - R&TTE Compliance Statement

About This User's Manual

This manual is mainly designed for, but not limited to, the following hardware and firmware for the IE-WL-AP-BR-CL-ABG:

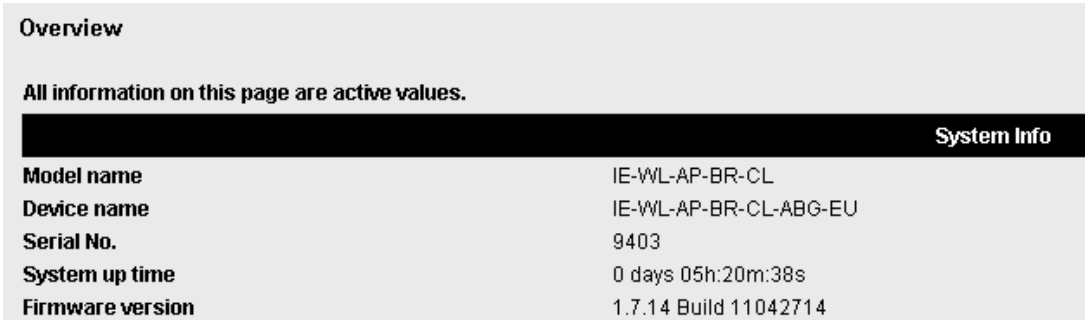
- Hardware Rev: **1.2**
- Firmware Ver: **1.7**

You are strongly recommended to visit Weidmüller's website (http:// www.Weidmueller.com/Downloads) and find the latest product datasheet, firmware, HIG (Hardware Installation Guide), User's Manual and related information.

NOTE

You can find out the hardware revision number of IE-WL-AP-BR-CL-ABG on the side label of the device.

The firmware version number can be seen on the **Overview** page, as follow:



DoC (Declaration of Conformity)

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution: To assure continued compliance, (example – use only shielded interface cables when connecting to computer or peripheral devices). Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment. This transmitter must not be co-located or operated in conjunction with any other antenna or transmitter.

FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 cm between the radiator & your body.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

FCC 15.407(e): Within the 5.15-5.25 GHz band, U-NII devices will be restricted to indoor operations to reduce any potential for harmful interference to co-channel MSS operations.

NOTE The availability of some specific channels and / or operational frequency bands are country dependent and are firmware programmed at the factory to match the intended destination. The firmware setting is not accessible by the end user.

R&TTE Compliance Statement

Weidmüller declares that the apparatus IE-WL-AP-BR-CL-ABG complies with the essential requirements and other relevant provisions of Directive 1999/5/EC.

This equipment complies with all the requirements of DIRECTIVE 1999/5/CE OF THE EUROPEAN PARLIAMENT AND THE COUNCIL OF 9 March 1999 on radio equipment and telecommunication terminal equipment and the mutual recognition of their conformity (R&TTE).

The R&TTE Directive repeals and replaces in the directive 98/13/EEC (Telecommunications Terminal Equipment and Satellite Earth Station Equipment) as of April 8, 2000.

Safety

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this and of the computer manufacturer must therefore be allowed at all times to ensure the safe use of the equipment.

EU Countries Intended for Use

The ETSI version of this device is intended for home and office use in Austria, Belgium, Denmark, Finland, France (with Frequency channel restrictions), Germany, Greece, Ireland, Italy, Luxembourg, Portugal, Spain, Sweden, The Netherlands, and United Kingdom.

The ETSI version of this device is also authorized for use in EFTA member states Norway and Switzerland.

EU Countries Not Intended for Use

None.

Potential Restrictive Use

France: only channels 10, 11, 12, and 13.